The Leader in Voting Technology

Contra Costa County Shadow Election Report

During five days, from October 30th to November 3rd in 2000, Safevote conducted an official public election precinct-based Internet voting test in Contra Costa County, under contract with the Secretary of State of California.

The number of voters who participated in the test, at will, was typical of the number of voters that would usually vote in one precinct in California, with 307 voters using the Safevote system. The test was done at one location using one voting station, which was online with Safevote servers elsewhere. Another voting station was also online but as a back-up.

Safevote used common PCs from a leading manufacturer, provided by Contra Costa County, with Safevote's custom-installed election system software. A LEO (Local Election Official) verified that all PCs and software were working as desired, before the polls opened.

A first station, called the LEO station, was used off-line to generate a DVC™ (Digital Vote Certificate, see DVC articles in the FAQ "Election Products" category, at the Support Center) for each voter, by a LEO. The voter's eligibility was first verified by the LEO. The LEO could not see the DVC that was given to the voter. Once the voter was authorized by the LEO, the voter's ballot style according to district of residence (a total of 280 ballot styles were possible for Contra Costa County), as well as a password chosen by the voter, were used by the Safevote software in the LEO station to generate the DVC. The DVC value was unpredictable and unknown to anyone but the voter; the length of the DVC and the password were enough to thwart any attempt to guess their combined value for the test conditions at hand.

For auditing and tallying authorization purposes, the name of the LEO authorizing the DVC to be issued, as well the ballot style, time, date and other information (but not the DVC value itself), were encrypted and recorded. LEOs could not influence the value of the DVC and could not create more than one DVC per voter. There was no connection whatsoever between the LEO station and the test network with the voting station where the voter would vote. The DVCs were accepted or rejected by the voting station based solely on the DVC's off-line properties as digital certificates, authenticating both the voter and the ballot style that was previously authorized off-line by the LEO for the voter.

To use the system, voters sign onto a voting station using their unique DVCs and passwords, allowing complete voter privacy when voting, and also providing for election integrity. There was no password list or DVC list in the voting station or anywhere else. In the test, 140 different ballot styles were actually assigned to voters based on their addresses in the county, and 100% correctly authenticated during voting. That each voter was using their correct ballot style, could be directly verified by the voter herself, providing an added assurance to the voter that the voter was correctly authenticated by entering their DVC and password. A similar process is used by Safevote also in online voting, to prevent phishing, spoofing and other authentication attacks.

The DVC authenticates not only the eligibility of the voter, thus preventing someone from voting twice, but also defines by cryptographic authentication the ballot style authorized by the LEO for each voter. The DVC also provides other cryptographic proofs in various stages of voter authentication, ballot casting, and auditing. The voter used either a mouse or a touch screen to make selections to vote. The touch screen was, clearly, the best device for voter input, specially for the elderly and computer novice.

The ballots cast by voters were encrypted and digitally certified. The precinct voting station did not have to be online with the Internet for the voter to vote. The encrypted ballots cast by voters were stored locally, using a "store and forward" mechanism to send them to a set of remote ballot boxes (i.e.,secure servers on the Internet). Without an Internet connection, the precinct voting station could work as an electronic voting system, and it could have operated in such mode exclusively. The Safevote precinct network was in "stealth mode" on the Internet: It could "see and talk" but could not be seen by anyone on the Internet -- including attackers. The names of candidates, or issue numbers, were not available in the cast ballots. There is a certified association between a candidate name and a tallied result but, to allay concerns of internal fraud, it only occurs in the Safevote system after all ballots are tallied. The key to decrypt the ballots was also not available in the system -- to obtain it, one would have to first decrypt the audit log for DVC issuance, which would immediately stop the DVC issuance. Tallying was done after the U.S. November 2000 election was officially over in California, as authorized by the Secretary of State. Before this event, the ballots cast could not be opened, read, or tampered with. Even if they would be opened, they could not be tallied to obtain a useful result, as the names of options chosen by voters (actual candidate names and issues) are not recorded in the ballots.

Voters could, and did, verify that their ballots were received at the remote ballot boxes by visiting a Safevote-run Web service with voter lists for *cast ballots received* (in addition to voter lists for showing up for voting). Verifiability can considerably reduce the probability of undetected fraud. If only a small fraction of voters do verify that their cast ballots were indeed received for tallying, voters in the entire election will benefit because this process reduces the probability of errors and undetected fraud, for example, of ballots being lost.

In the first days of the test, from October 30th to November 1st, the test was dedicated to experiment with the failure modes of the Internet voting system developed by Safevote. Public voting systems need fail-safe assurances and they need to be test crashed in order to see if they indeed are fail-safe. During this initial period, 161 voters cast ballots that were on purpose deleted for testing the failure modes of the system. The presence of these voters, however, was detected by several verification loops built into the system audit, including the public voter list verification service made available on the Internet by Safevote. Contra Costa voters visited the voter list and tested if their participation was recorded, from their computers in homes or offices. Safevote observed thus that voters really care enough to both verify the voter list and notify Safevote about

any problem, even though this was a shadow election. This exemplifies that this mechanism can be quite effective to enhance security in a real election. Voter privacy was not compromised by this verification procedure.

From November 2nd to November 3rd, all voted ballots were kept, encrypted, with the assurances aforementioned. Voters could and did verify remotely on the Internet that their ballots were received for tallying. Voter privacy was not compromised by this verification procedure.

During the five days of the test, Safevote also conducted a public attack test, concurrently. This was the first -- and only so far -- time that an Internet voting company made a public invitation to attack their own system.

The Safevote attack challenge was made public on CBS, USA Today, Internet lists and other public media, so that attackers would be motivated to try to attack. No one managed to successfully attack the system, which was on the public Internet for five days and 24-hours per day, in spite of an attack-hotline with phone, email and web-page support, and time-saving hints provided by Safevote. Attackers were also encouraged to submit theoretical attacks on the data structures used, not just the networks. Denial-of-Service attacks were also tried, as reported at the attack web-page. No attack was successful. The Internet access used by Safevote was provided in dial-up and the attack test never put the election office network in Contra Costa County at any risk whatsoever.

Of course, security cannot be proven by any amount of tests. The objective of an attack test such as the one performed by Safevote at Contra Costa County must be to find problems, not to prove that problems do not exist. However, the absence of both theoretically successful attacks as well as practical attacks during an extended period of time in a high-visibility open test with attack assistance and feedback, and the absence of any successful attack in six years of operation with over 100 elections, suggests that the technology used by Safevote does offer a noticeable security increase over a typical e-commerce system.

On November 7th, 2000, the results were audited and tallied after the official election closed. All the results were authorized to be shown by Safevote but not verified by the office of the California Secretary of State. A total of 146 valid ballots were tallied, with 161 test ballots, for a sum of 307 ballots.

Voting test results at Contra Costa County Shadow Election 2000 >>

Contra Costa County Ballot Survey

In the Contra Costa County Shadow Election, voter feedback about the test and the possibilities of voting using the Internet, including voting from home, was even more important than knowing the voter's political preferences.

A Safevote representative personally interviewed the voters at Contra Costa after they voted using the Safevote system and presented a series of questions to them. When asked if Safevote's system was easy to use, all 307 voters answered yes. As voters' time permitted, other questions followed with a pre-defined format and also included room for spontaneous responses. Approximately 200 voters took the time to answer all questions, with the results given below.

- **Ease of Use:** 100% of 307 voters found the Safevote system easy to use
- **Sensitivity to Privacy and Security Issues:** (high level of awareness)
  - 70% said they had concerns about security
  - 20% said they had concerns about voter authentication
  - 60% had concerns about voter privacy
- **Vote Verifiability:** 100% would like to go on the Internet and verify that their vote was indeed received for tallying
- **Would You Use the Internet to Vote:** (nearly 100% said yes)
  - 60% would vote from home
  - 34% would prefer to vote from the workplace
  - 5% would prefer to use the Internet to vote at precincts
  - 1% did try the system even though they declared they were completely opposed to the idea of Internet voting

The observed high level of awareness of privacy and security issues among the voters correlated well with their desire to verify whether their ballots were actually received for tallying, as aforementioned. The voters' high level of awareness of privacy and security issues indicates that voters might be well-motivated to cooperate in providing the voter-verified part of the checks and balances called for in Safevote's Election Auditing technology.

Public Elections

Safevote stands ready to certify and conduct Internet and electronic voting in Public Elections, where accepted. Where the certification of Safevote's system depends on legislation still being discussed, Safevote is able to conduct Public Election Trials.

If you are interested in setting up a Public Election or Trial, please visit our Public Elections Page >>

Shortcut Text	Internet Address
	http://safevote.com/index.html
Products	http://safevote.com/products.htm
Request Quote	http://safevote.com/quote.htm
Support Center	http://safevote.com/support.htm
Contact Us	http://safevote.com/contactus.htm
Election Requirements	http://safevote.com/requirements.htm
Partners	http://safevote.com/partners.htm
About Us	http://safevote.com/aboutus.htm
Public Elections	http://safevote.com/public_elections.htm
Licensing	http://safevote.com/products.htm#Licensing
Reliability in Voting	http://safevote.com/doc/VotingSystems_FromArtToScience.pdf
Voting Requirements	http://safevote.com/doc/vote-req.pdf
Fail-Safe Voter Privacy	http://safevote.com/doc/thebell1.8.pdf
Contra Costa County	http://safevote.com/onlineballot.htm
Ballot Survey	http://safevote.com/surveyballot.htm
Witness Voting System	http://safevote.com/doc/gerck-witness.pdf
E-Government	http://safevote.com/doc/UNEG-Palermo-02.PDF
Available by request:	http://safevote.com/reports.htm
Information Center	http://safevote.com/information.htm
The Bell Newsletter	http://safevote.com/TheBell.htm
Free Small Elections	http://safevote.com/free.htm
Employment	http://safevote.com/employment.htm
Press	http://safevote.com/press.htm
Legal Statement	http://safevote.com/legal.htm
Privacy Statement	http://safevote.com/legal.htm#YOUR_PRIVACY
Contra Costa County Shadow Election 2000 >>	http://safevote.com/evote/
Election Auditing	http://safevote.com/requirements.htm#A