☑ Computer Professionals for Social Responsibility Turns to Internet Voting

Deliberate.Com
Mountain View, CA

June 29, 2006

Computer Professionals for Social Responsibility, after years of warning against paperless electronic voting, is experimenting with an Internet-based open-source voting system, ***eVote***®, for its annual board elections this year.

The group is quick to point out that this action serves to open technical discussion about open-source Internet voting and does not conflict with their recommendation to government:

> CPSR does not endorse the use of electronic voting without a paper audit trail for government elections, including municipal, state, and national elections. As a nonprofit organization with a small budget, however, we believe online voting is a cost-effective way to encourage the greatest number of our members to vote. Our choice reflects our belief that electronic voting without a paper trail should only be used in an extremely limited context. This limited context does not include political or government elections.

Even so, the system CPSR chose to try, eVote®, being an Internet-based solution (in contrast to the voting-booth electronic systems currently in use) brings a new set of considerations to the discussion about electronic voting. In general, electronic voting is criticized for the following points which are ***not*** applicable to the CPSR eVote® system:

1. Once the ballots are counted, they are gone and no recount is possible.

   > This is true for the paperless voting-booth machines, but the Internet-based solution chosen by CPSR keeps the ballot, and, before the poll closes, the ballot is available to the voter for changing the vote, and after the poll closes, for checking and re-checking.

2. Electronic voting can be done very badly in a myriad of ways.

   > This is true, and frightening. But also, electronic voting can be done in an open, and redundantly-checked way that emulates a show-of-hands. eVote® allows voters to see and change their votes until the poll closes; and once the poll is closed, everyone can see all the ballots. Recounts are almost free. There is no way to cheat in such an election.

3. You cannot use the Internet for voting because of denial-of-service (DOS) and man-in-the-middle (MIM) attacks.

> Yes, the World Wide Web is vulnerable to DOS, or network floods, that render a web site useless; but the email conduit is flexible and sturdy under attack. When an email server is attacked, its incoming email waits for the server to catch up from the the attack.
>
> And, yes, MIM is theoretically possible to maintain in a limited way for a very short period, but the voter's ballot is available for changing and fixing for much longer, and for checking even after the poll closes.
>
> When using email to transmit ballots and send vote receipts, when things break, people aren't inconvenienced except that their vote receipt takes a little longer to get back to them. CPSR's solution uses email to transmit ballots from the voter to the server, and email to transmit vote receipts back to the voter.

For convenience, the CPSR eVote® system also provides a web page for voting that generates the ballot from the voter's choices and sends it by email.

Vote Privacy

Anonymity for CPSR voters was designed into the system by giving each voter a temporary email address with a coded name like RKEOoX6YB3jg4qO2oC26LHn8KJ3BLR86@maildance.com. Voter privacy is maintained by distributing the email-address codes to voters in some random way, like shuffling and dealing cards.

The vote system does not know, indeed no one knows, which voter has which code. Each voter only knows their own code. Therefore, the ballots can be displayed for everyone to see. Everyone can check their own vote; everyone can tally the votes.

For this election, the CPSR office does keep a record of which voter has which code for two reasons: to be able to help voters with this new process; and to keep the voters honest after the poll closes. After the poll is closed and all the ballots, votes and codes are revealed, any member could claim to be the owner of any email-address code, forge a receipt, and further claim that their vote was recorded incorrectly.

In the future, a Message Authentication Code (MAC) will be added to each emailed receipt so that vote receipts cannot be forged. A MAC is a small addendum to a message that, when paired mathematically with a secret key, proves that the message has, or has not, been altered. Since only the vote

administrator has the secret key, only the vote administrator can prove if a receipt was forged or not, and there is no reason to keep a record of which voter has which email-address code. Voter privacy is entirely in the voter's own hands.

Flaws

CPSR's eVote® system did not encrypt the email ballots. Therefore, a voter's privacy can be breached by attaching a sniffing device on the phone line near the voter's computer. Encryption technology for solving this problem is well-developed. But for the CPSR election, the risk is not considered to be worth the effort of adding encryption.

CPSR's eVote® system does not prevent voters from revealing their ballots to someone else. This, the only flaw seen (so far) in an open-vote system, means it is technically possible to buy/sell a vote. This flaw is also present with absentee voting through the postal mail.

Conclusion

There is a trade-off of dangers between open voting on the Internet and voting in a voting booth:

☑ Open voting on the Internet, while it provides absolute accuracy, and global accessibility, also offers the technical possibility of vote-buying. This danger, however, can be rendered impractical by giving a financial reward for information that leads to the arrest and conviction of a vote-buyer.

☒ With voting in booths, accuracy is always in doubt. Recounts, if possible, are very expensive. Fraud can be revealed years after a bogus election put criminals in public office.

Robert Guerra, CPSR director, looks to the future saying, “Constructive comments both on the process and the code itself are VERY welcome. .... As for next steps- the results, methods and comments received will be collated, reviewed and a summary report written. The call will hopefully yield a set of recommendations that will help CPSR plan and stage its next election.”

eVote® is open-source software available at SourceForge.net provided by Deliberate.Com.

Contact:
Marilyn Davis
(650) 965-7121
marilyn@deliberate.com