IS ELECTRONIC VOTING (e-Vote) SAFE ?

by D Allan Sangster BScEng MIEAust CPEng MCIRCEA
from Sangster Telecommunications Pty Ltd

The purpose of this article is to encourage discussion of Safe Electronic Voting. The aim is to check that e-vote quality is at least as good as the paper voting it replaces. A comparison may be obtained by giving each voter the choice of using electronic or paper voting and comparing the end results. A difference of more than 4% between electronic and paper % vote results, indicates a possible problem and need for closer checking. Also, there is no need to change an existing electronic voting system to identify problems, simply monitor performance e.g. as shown in the Paper v/s e-Vote Comparison shown below.

Vote Over Internet

Organisations using the Internet for electronic voting can get Australia wide coverage, low cost and voter convenience. Unfortunately they also expose the actual voting process to cyber attacks by computer hackers. This is when a 17 year old schoolboy on the other side of the world, accesses a supposedly impregnable computer and makes changes which corrupt the central computer system e.g. embed foreign code or alter data. Similar examples are quoted in the news media every few weeks. Also, Certification that e-Vote system designs meet Guidlines for handling known problems, does not help when an unpredictable/unknown problem cyber attack occurs over the Internet.

New Process

Internet electronic voting is a new process and many new e-Vote systems have been designed. These range from highly protected and Verifiable Internet voting systems; complicated for the voter and limited to a few thousand votes - through to poorly protected systems; easy for voters to use and low cost. Therefore an in-depth professional engineering analysis based on fundamental principles is necessary. This analysis helps select a safe system that can meet the requirements of the Australian Corporations Act and the Organisation's Constitution e.g. 100,000 member Engineers Australia Royal Charter and By-Laws. If a suitable system cannot be found then do not use electronic voting !!

Pre-voting stage	Cast vote-typical 1 month	Post-voting stage
Testing/Certification/Audit		Audit/ProcessValidation

OUTLINE OF e-VOTING FOCUS

Worldwide e-Vote Search

A Google search shows a focus on Certification to Guidlines, using audit/testing/monitoring of e-voting systems. This Certification occurs before the Ballot (e-vote) and after the Ballot (e-vote), but nothing occurs during the Ballot i.e. "cast vote" or "casting of the vote" stage. This means that vote corruption by innovative Hackers during the "cast vote" stage may easily go unnoticed. Thus no redesign of systems to overcome an unknown problems is possible. In my opinion a report on patterns of corruption and inconsistencies during the actual Ballot is required (see Monitoring Ballot Vigilance below). This is because the post-voting stage (process validation and audit) do not show if such vote corruption has occurred.
Also particularly in Europe, focus is on Accredited Election Observers (Scrutineers) having access to all steps of the certification process with transparency of all reports and avoidance of non-disclosure agreements.

POLLING BOOTH

A key issue for electronic voting is whether a Polling Booth is used. Without a Polling Booth, an independent body posting information to the home address of Members is considered an essential check on the Electoral Roll, but it is expensive. Unfortunately, even Verifiable Internet voting systems do not check if the Electoral Roll is correct. Return of the undelivered letters provides an independent check for bogus members e.g. 1000 returned letters and 1000 similar votes from the same IP address indicates serious fraud.

WITH POLLING BOOTH (electronic voters must visit a polling booth)

1. Electoral officials have close supervision of voters. For example if using Polling Booth computers, then this minimises the chance of Computer Hacking by an onsite voter.
2. Voters have to physically attend and have their name crossed off list. This minimises chance of bogus Members voting. Also no need to send a secret key out to each Member.
3. Use of a private computer Network (No public Internet use), minimises Computer Hacking over the Internet by an offsite person.

WIHOUT POLLING BOOTH (electronic voters vote remotely on their own computer)

1. No close supervision of voter activity. High risk of Computer Hacking/Voter Fraud by a voter.
2. Public Internet used. High risk of Cyber attack by a Computer Hacker corrupting votes.
3. POST (by independent official), confidential key to each Member. Undelivered mail returned to these officials can raise alarm on Bogus Members. OR
4. EMAIL confidential key to Membership list. Difficulty detecting bogus members means a high risk of Voter Fraud. Analysis of actual vote IP address patterns can indicate a problem.

Monitoring Ballot/Vigilance

Simulated tests with sample data are inadequate because real life conditions are unpredictable. The validity and integrity of every ballot should be assessed by using checks on the live electronic/internet ballot vote, with oversight by Scrutineers. Vigilance checks include the Ballot Computer monitoring and recording its own activities. Such monitoring processes and devices are well established and low cost and include encrypted recording of Hash Keys (of programs and Electoral Roll), IP addresses, agent strings, central Ballot computer activities etc.. These results may then be checked for patterns of corruption and inconsistencies. Such vigilance and feedback to voters provides voter confidence in the process and helps identify problems, but does not fix the problems.

Engineering Guidelines Help Fix Problems

Evolution of engineering guidelines and standards for e-voting (i.e. specification, testing, commissioning, monitoring, and operations management) will help drive improvements in future electronic voting systems and help manage risk. Also a useful benchmark for guidelines is the Australian Federal, State and Local Government Election (paper vote/Polling Booth) procedures with Scrutineer oversight.

Feedback To Voters

Transparent procedures may be used to identify problems and improve the electronic voting system.
Also providing feedback to Scrutineers and voters will give them reassurance that the Ballot system integrity is improving and not going backwards. It also helps if an open and transparent system is applied generally, such as candidates nominating Scrutineers; posting secret keys to voters; not opening votes until voting closes; Scrutineers given vote totals (i.e. main, preference, electronic and postal); a completely independent returning officer and equal promotion of all candidates and/or issues.

ELECTRONIC VOTING

Generally electronic voting attempts to follow the well-established basic principles of paper voting. However higher security is sought because a small normal error can affect a few paper votes but a small computer error can affect many thousands of electronic votes. My Scrutineer experience is that the risk of distorted Ballot results from unsafe votes, seems to increase when changing from paper to electronic votes. Also some protection against computer hackers is normally attempted, by engaging a good "White Hat" hacker to try and breach your computer security, and then plugging any gaps found.

- **Paper V/S e-Vote Comparison**

PAPER PROCEDURES	ELECTRONIC PROCEDURES
A. PAPER VOTING - POSTAL VOTES Post papers to each voter home postal address Returned mail - voters removed from Electoral Roll. SCRUTINEERS present for opening/counting votes and are given totals - primary votes & preferences.	C. ELECTRONIC VOTING - EMAIL INTERNET Post secret Token to each voter home postal address. Do not send token with email of voting instructions. Australia Post returned mail - voter may be deceased? Electoral officials remove this voter from Electoral Roll. continue as below
B. PAPER VOTING - POLLING BOOTH Voter visits local Polling Booth, makes paper vote SCRUTINEER present for SEALING & UNSEALING SEALING - View ballot box is empty before sealing. Electoral staff check and set up electoral roll. Electoral staff monitor all Polling Booth activity. Voting - Electoral staff check electoral roll for voter, voting paper issued, voter completes & puts in Ballot Box. UNSEALING Scrutineers enter and Polling Booth is locked. Ballot Box seals are unsealed. Ballot Box is emptied in Scrutineer presence. Scrutineers witness vote counting. Scrutineers are given totals - votes & preferences.	ELECTRONIC VOTING - POLLING COMPUTER Voter accesses remote Polling computer via Internet. SCRUTINEER present for 'checks and balances". Empty Log file - overwrite file by loading "erase file". Load electoral roll into computer memory & seal records. Total computer activity record on sealed WORM memory Seal "Checksum" which checks Program is unaltered. Polling Computer - Program checks voter validity. electronic vote submitted is then processed/stored. Scrutineers enter locked computer room and watch. Unseal Log file, electoral roll, WORM & Checksum. Records downloaded, decrypted and printed as required. Votes counted electronically or manually as appropriate. Scrutineers given all totals - both electronic and paper.

CONCLUSION

Generally an open and transparent e-Vote process is considered safe if suitable independent scrutiny is carried out. However, if the e-Vote central computer is connected to Internet, then more extensive controls and scrutiny are required to handle Cyber-attacks. Unfortunately, because Cyber Security is so technical, Directors and Senior Executives don't take responsibility.

For example a computer Hacker may insert a small foreign code which changes incoming votes sufficient to change the election result. If this code is inserted after voting opens and removed before voting closes, then no one will know that the vote has been corrupted. Therefore Senior Executives must be persuaded that - with Internet connection, extensive scrutiny and monitoring of the central computer is required before, during and after the vote.

REFERENCES/Bibliography

Certification of e-voting systems - Strasbourg 16 February 2011 - Council of Europe
Introducing Electronic Voting: Essential Considerations - Policy Paper December 2011 - IDEA Stockholm, Sweden
http://harvardmagazine.com/2010/05/secret-ballots-verifiable-votes, Harvard Boston USA
Replay attacks that violate ballot secrecy in Helios - Ben Smyth May 10 2012 - Toshiba Corp Kawasaki, Japan