CORE Submission to the Inquiry into the 2007 Federal Election

The Computing Research and Education Association of Australasia, CORE, is an association of university departments of computer science in Australia and New Zealand. Its website is www.core.edu.au. This submission has been authorised by CORE's president.

This submission is written by Dr. Vanessa Teague on behalf of CORE. Dr. Teague is a former lecturer in, and soon to be an adjunct member of, the department of computer science and software engineering at the University of Melbourne. Her background is in cryptography and her research area is secure electronic voting systems.

This submission addresses the transparency and security of the electronic voting systems that were used in the 2007 federal election.

Electronic voting

The problem

Transparency is a fundamental requirement of elections. Not only must the count be correct, it must be conducted so openly that everyone agrees on the outcome. That is what elections are for. There is no inherent reason why electronic elections should be less transparent than paper ones.

Australians are rightly accustomed to trusting the AEC to handle paper ballots securely, but this trust follows from the transparency of the process: candidates and voters know that scrutineers representing their interests may be present at all stages of the count. Electronic voting requires much more trust, but in Australia has no scrutineers at all. Not only must the voter trust the programmers, the providers of the computers, and the auditors (none of whom are direct AEC employees) to act in good faith, but they must trust them not to make any serious mistakes. Writing secure software is notoriously difficult, as is checking it. A certification by a single auditor, however diligent, is no substitute for wider scrutiny.

If security holes exist, they could allow a hacker (whether an insider, a passerby, or a voter) to run a program that violated a voter's privacy or cast a vote other than what the voter intended. This sort of tampering might be undetectable and might affect the outcome of the election.

Main Recommendation

My main recommendation is that electronic voting should have similar transparency requirements to paper-based voting. In particular:

1. Whenever possible, the voter should have direct verification that their vote was cast as they intended and included correctly in the count (this is particularly difficult for visually-impaired voters, but see below), and
2. The auditor's report should be public, and the source code should be available to a much wider group of experts for analysis.

Detailed comments

The AEC trialled two very different electronic voting systems in the 2007 election. The first one, based on the eVacs system used in the ACT, allowed visually-impaired people to vote via a computer in the ballot box, without requiring assistance from a person. The second part of this submission makes one important suggestion for improving the security of this system, but otherwise I do not have serious concerns. By contrast, the second trial, which allowed overseas military personnel to vote over the Defence Department's intranet, raises very serious security concerns.

Remote voting for defence department personnel

Remote electronic voting suffers from the same problems of vote-buying, coercion and privacy invasions as postal voting, plus electronic attacks such as viruses, worms and phishing. An apparently very similar US system (called SERVE) was cancelled just before deployment when a panel of independent security experts found "numerous … fundamental security problems." [1]. Since the details of the AEC's scheme are secret, nobody can guarantee it doesn't have similar

security problems. It is not good enough that there exists a secret report by an auditor who says they checked for some vulnerabilities. The short summary of this report on the AEC's website makes no reference to SERVE and provides no convincing explanation of why the system should be trusted.

The AEC claims to provide some verification to voters:

"Once a vote has been cast, a personal receipt will be generated. ADF members will have the ability to verify online whether their vote has been successfully cast using their personal receipt."[2].

Such verification is an important part of any well-designed system, but it is valuable only if it, too, is behaving as expected. Otherwise, a hacker who broke into the system, or an accidental programming error, could cause the verification step to fail as well as the vote-casting step. Furthermore, the voter can't verify that the *correct* vote was received or counted, only that *some* vote was received. (Of course I am not suggesting the website should report how a person voted, because this would expose them to coercion and vote-buying.) This is far less verification than the AEC offers with traditional paper ballots, even postal ones.

As a scrutineer in the last election, I asked the AEC for permission to observe this system. I was told there was no opportunity for scrutineers to do so. I have repeatedly asked to read the auditor's report, on which public trust in the system is supposed to depend. Although the AEC website states that the report is available online, neither hours of searching nor repeated requests to the AEC have actually elicited more than a one-page "executive summary". The almost-total absence of any public information about this system is unacceptable for a public election. Secrecy does not engender trust.

Computerised ballot-box voting for visually-impaired voters

Visually impaired voters were able to vote privately via a computer in a pre-polling station. Previously they had had to use more cumbersome technology, or rely on a sighted person to cast their vote. I was able to observe this system at two locations in Victoria (though of course I did not observe people actually voting). The design is based on the eVacs system used in the ACT, though its source code is secret while that of eVacs is public. The voter tells their vote to the computer, which then prints out a barcode representing the vote, which the voter then places in a declaration envelope. The barcode is not readable by a human, so even voters who need help with the declaration envelope maintain their privacy.

It is important to realise that this system does not have a true voter-verifiable paper audit trail, an issue discussed in detail in my submission to the Inquiry into the last Victorian state election [3]. The main point is that, if the computer malfunctioned, it would be impossible for voters (or polling station officials) to detect that the printed barcode was incorrect. This would be true even for sighted voters, because the barcodes are not human-readable. Furthermore, any malfunction that was somehow detected would be impossible to correct after the election without violating the privacy of those voters who had used the computer. There is a very simple way to improve this situation considerably: the machine's output should be regularly audited *throughout the voting period*. Officials (at least two working together) should commence a normal voting session[1], cast a valid vote, print it out in barcode form, then put it in a special envelope which is marked "test" and

[1] It is important that the computer has no information about whether this is a genuine vote or a test, but of course this is not the true vote of the officials, whose privacy would be violated if it were.

also contains a signed statement of which vote was supposed to be cast. Scrutineers and voters should be allowed to observe this process. The test envelopes should be opened, and the barcode's correctness verified, in some public way, possibly at the polling station, and/or at the same time and place the other declaration votes are counted. (Of course this is no defence against a hacker who tampers with the barcode reader, but it would detect malicious modification of the voting computer only.) This could significantly improve voters' confidence that the machine was printing the vote they intended.

Conclusion

No useful system, electronic or otherwise, is perfectly secure. However, security can be improved by transparency, exemplified by the presence of scrutineers throughout the counting of paper ballots. We would never consider evicting the scrutineers and replacing them with a single auditor who was paid to certify a secret counting process, yet that is exactly what happened with electronic voting in the last election.

Giving the software a security audit before the election is a good way of improving its quality, but again I emphasize that this provides no absolute guarantees. Just as no system is perfectly secure, no auditor does perfect security analysis. I believe that the source code should be made available to more than one group of experts for analysis. Even then, a security audit cannot guarantee that the program running on the computer is exactly the one that has been audited. Regular testing of the system for visually impaired voters throughout the voting period would improve its security considerably. With no information about the system for overseas military personnel, it is impossible to make concrete recommendations, except to say that it is not acceptable for votes to be inserted into the tally without adequate scrutiny.

References

1. D. Jefferson, A. Rubin, B. Simons and D. Wagner, 2007. SERVE security report, www.servesecurityreport.org
2. AEC website, http://www.aec.gov.au/Voting/e_voting/adf.htm
3. V. Teague, 2007. CORE submission to the Inquiry into the 2006 Victorian state election, submission 26. http://www.parliament.vic.gov.au/emc/2006%20State%20Election/Submissions/26_CORE.pdf

Contact details

Dr Vanessa Teague
vteague@csse.unimelb.edu.au

Declaration

My husband was an independent candidate for the Senate in the 2007 Federal election. It was as his scrutineer that I was able to observe the electronic voting process for visually impaired voters.