COmputing Research & Education

Submission to the electoral matters committee inquiry into voter participation and informal voting

This submission examines the security of electronic voting machines in ballot boxes. We recommend that, if electronic voting is extended to voters who can read paper printouts, the system should include a voter-verifiable paper trail, or some other form of direct verification by voters.

This submission is very similar to CORE's submission to the inquiry into the 2006 Victorian State Election (submission 26).

The Computing Research and Education Association of Australasia, CORE, is an association of university departments of computer science in Australia and New Zealand. This submission is endorsed by CORE's president, Prof Justin Zobel.

The author is Dr Vanessa Teague, an honorary fellow in the department of Computer Science and Software Engineering at the University of Melbourne. Dr Teague's research focuses on electronic voting security. She would be happy to discuss these matters further with the committee, and can be contacted by phone on 8344 1274 or by email at vteague@csse.unimelb.edu.au.

COMPUTING RESEARCH & EDUCATION
ABN 79 455 832 902
C/o Department of Computer Science & Software Engineering
The University of Melbourne, Vic, 3010

Main Recommendations

1. **If electronic voting is extended to voters who can read their own printout, then it should provide a printout for them to verify (a voter-verifiable paper trail), or some other form of direct verification.**
2. **The auditor's report should be public, and the source code should be available to a much wider group of experts for analysis.**
3. **There should be an Australia-wide set of standards for electronic voting systems, and it should include points (1) and (2).**

Verifiable Voting

The electronic voting machines trialled in the last Victorian election made only electronic records of the votes cast. Voters were of course unable to verify the electronic records directly, so were given no absolute guarantee that the computers recorded their votes as they intended. They had to trust the software that had made the record to "read it back" to them truthfully. This is not the same as seeing a paper ballot put into a ballot box. This problem has been widely recognized by security and voting experts [1,6].

Electronic voting machines that do not allow the voter to verify their vote do not provide any useful way of resolving disputes. A disappointed candidate could legitimately question whether the machines had recorded the votes as the voters wanted. Even if the machines were perfectly secure and recorded every vote perfectly, there would be no evidence after the election that this was so. Allowing the voter to verify their vote solves this problem.

A voter-verifiable paper trail

A true voter-verifiable paper trail would work as follows. First the voter would interact with the computer in the ballot box, choosing how they wanted to vote. There could then be a visual or auditory checking phase. Finally, after the voter was satisfied that they had expressed their intention correctly, the computer would print a ballot that the voter could read but not touch. The voter would be asked (again) to check the vote, then if the voter accepted it it would be deposited into a ballot box. If the voter did not accept it, it would be shredded and the voter could start again. This would produce a paper trail that could be used to check the results and resolve disputes after the election. The paper trail would not normally be used for initial

counting, so results would be available just as quickly and cheaply as in an all-electronic system. It would be a great way to increase voter confidence in electronic voting, because voters would be able to see that those recounts that were conducted agreed closely with the electronic count.

Computers that produce completed ballots

An alternative design is to use the computer simply as a tool to help the voter print a ballot, which the voter would check before placing it in a ballot box or declaration envelope. Although this design may be inappropriate for visually or motor-impaired voters, it provides a simple, verifiable system that might work well for some voters, such as those whose literacy in English is poor.

The system for visually impaired voters trialled in the last Australian Federal election had a similar design, though the printout consisted of a barcode which humans could not read. Obviously this feature was deliberately included to preserve the privacy of those voters who needed help taking their printout off the printer and putting it in the declaration envelope. We recommended that, if the system was extended to voters who could read their own printout and put it in the envelope, it should have an option to print a human-readable vote. We also recommended that the barcode printouts be checked throughout the election [3].

Other forms of verified voting

There are cryptographic schemes for electronic voting that aim to achieve a higher level of security than paper-based schemes. Their main advantage is a very strong form of verifiability: voters can check that their vote was cast as they intended, that it was included in the count, and that the tally is correct. These schemes generally work by issuing an encrypted receipt to each voter, which does not reveal how the person voted, but does allow them to check that their vote was counted. Although these schemes are extremely promising, we know of none that has all the security properties and functionality required for Australian elections. (The Prêt à Voter scheme [2,4,7] and the VAV scheme [5] both have many of the features we need.) Designing such a scheme, or modifying existing schemes to incorporate Australian voting, is the main focus of Vanessa Teague's research.

It is important for the wording of any legislation not to preclude these sorts of systems. It would be enough to require that voters can verify that their vote was cast as they intended, without having to trust the software.

The current situation in Victoria

Victorians are rightly accustomed to trusting the VEC to handle paper ballots securely, but all-electronic voting requires much more trust. Not only must the voter trust the programmers, the providers of the computers, and the auditors (none of whom are direct VEC 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. Security holes could allow a hacker (whether an insider, a passerby, or a voter) to run a program that recorded a vote other than what the voter intended.

The VEC's current system has separate modules for recording the vote and for allowing the voter to query what has been recorded. This is a good way to test for accidental programming mistakes, but it does nothing for security. It is straightforward to write a program that records one value and then "reads back" to the voter a different value. The fundamental problem is that it is impossible for a voter to test whether the software running on the computer is doing what the voter expects.

A voter-verifiable paper trail was recommended by the 2005 Scrutiny of Acts and Regulations Committee report on Victorian Electronic Democracy (Recommendation 53), but when the relevant legislation was written in 2006 the requirement was weakened to allow the printing of ballots long after the close of polls. This achieves absolutely nothing for security, because the voter has no way of verifying that what is printed is what they wanted. We agree entirely with the VEC's recommendation that the electronic data be loaded directly onto the tallying computers.

Giving the software a security audit is another good way of improving its quality, but again we emphasize that this provides no absolute guarantees. Just as no system is perfectly secure, no auditor does perfect security analysis. We 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.

No useful system, electronic or otherwise, is perfectly secure. Even paper-based voting has an important set of protocols concerning the physical security of ballots, the privacy of the voting booth, *etc*. Electronic systems are the same – we must make some assumptions about the physical security of the computers, the privacy of the ballot boxes, and so on. We can then ask how hard it is for people in different roles to discover someone's vote or alter the outcome of the election. When considering a change, we should ask whether it makes certain kinds of security breaches easier or harder. For example, visually impaired voters have had neither privacy nor verifiability in the past, because they have had to tell their vote to another person and trust that person to cast it as they instructed. Hence an electronic voting system that provides privacy without verifiability is arguably an improvement. However, the VEC recommends extending electronic voting to people such as motor impaired and non-English speaking voters, who currently have verifiability but no privacy. For these voters, an electronic vote would give them privacy while taking away their verifiability. It is not clear that this is an improvement. If it provided them with both privacy and verifiability, then this would be unequivocally better.

Notes on other aspects of electronic voting

We support the VEC's recommendation of an Australia-wide set of standards for electronic voting systems. This would help the security analysis as well as increasing the ease of voting. We would be very happy to contribute. The United States' Election Assistance Commission is currently considering a set of standards [9] (which

are voluntary because the US federal government does not have authority over voting systems). Their current draft includes a strong requirement for voter-verifiability.

We agree with the VEC that introducing Internet voting in the near future is inadvisable due to security concerns.

Summary

Voters should have some way of testing that their vote is being cast as they intend. A voter-verifiable paper trail, allowing voters to check the printout at the time they cast their vote, would be one way to achieve this. While it may be pointless for visually-impaired voters, it is an important security feature for those who can read a printout.

References

1. ACM Statement on voting systems, Communications of the ACM, 47(10), October 2004.
2. D. Chaum, P. Ryan, S. Schneider, "*A practical, voter-verifiable election scheme*," Proc. European Symposium on Research in Computer Security (ESORICS) 2005, Springer Lecture Notes in Computer Science, vol 3679, pp. 118-139.
3. Computing Research and Education Association of Australasia (CORE), submission to the inquiry into the 2007 federal election (Submission 116).
4. J. Heather, "*Implementing STV securely in Prêt à Voter*," Proc. 20th IEEE Computer Security Foundations Workshop (CSF) 2007, pp. 157-169.
5. R. Rivest and W. Smith, "*Three Voting Protocols: ThreeBallot, VAV, and Twin,"*
   Proc. Electronic Voting Technology Workshop (EVT), Boston, MA, 2007.
6. R. Rivest and J. Wack, "*On the notion of "software independence" in voting systems*," http://vote.nist.gov/SI-in-voting.pdf
7. Z. Xia, S. Schneider, J. Heather, P.Y.A. Ryan, D. Lundin, R. Peel and P. Howard, "*Prêt à Voter: all in one,*" Proc. Workshop on Trustworthy Elections (WOTE), Ottawa, 2007.
8. Verified Voting Foundation. http://verifiedvotingfoundation.org
9. Voluntary Voting System Guidelines, United States Election Assistance Commission, http://www.eac.gov/voting systems/voluntary-voting-guidelines

COMPUTING RESEARCH & EDUCATION
ABN 79 455 832 902
C/o Department of Computer Science & Software Engineering
The University of Melbourne, Vic, 3010