COmputing
Research
& Education

Third 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 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 is CORE's third submission. It contains a summary of our recommendations and some specific suggestions about conducting electronic voting in the future. We thank the AEC for providing a demonstration of existing systems. This submission is a response to that demonstration and the ensuing discussion.

We would be very happy to discuss any of these issues further. The best way to contact Dr Teague is by email at vteague@csse.unimelb.edu.au. If necessary, other contact details are:

Telephone: (03) 8344 1274
Traditional Mail:
Department of Computer Science and Software Engineering
University of Melbourne
Victoria, 3010

Introduction

The usual Australian system of voting, whether in person at a polling station or remotely by postal vote, is carefully designed for privacy and transparency. The AEC's counting process is, as much as possible, made open to scrutineers so as to provide evidence of having produced the correct result. **Computerising voting can improve the experience for many voters, but this should occur only when the computerised system meets at least the same standards of privacy and transparency as the paper-based system it is replacing.** When computers are placed in the ballot box, and the software is designed with accountability as a priority, they can be as secure and accountable as paper-based voting (and sometimes even more so). Hence we support the continuation of the popular project to allow visually impaired voters to vote by computer in a ballot box, and we also support the extension of this program to voters with other impairments, as long as it provides them with evidence that it is recording the correct vote. This is described in more detail below. By contrast, we believe that, given current security infrastructure, designing remote networked voting to replicate the level of transparency provided by the postal system (which is itself imperfect) is "an essentially impossible task" [1]. Hence we recommend using the communications infrastructure in some way that doesn't require trusting software. This is not a criticism of Registries or Everyone Counts, who have demonstrated considerable technical expertise and attention to security and privacy. We know of no existing remote networked voting system that provides evidence of correctness comparable to the postal voting system. Further justification of this view, and some specific alternative suggestions, are provided below.

We recommend that there should be someone with technical security expertise in the reference groups for whichever projects go forward. This would allow security issues to be specified as requirements early in the process. There is a recent and rapidly-growing academic literature on the sorts of security properties that electronic voting systems should satisfy, and this would make a constructive contribution to the early stages of the project design.

Designing the system to provide evidence of recording the correct vote and producing the correct results sidesteps the controversial issue of exactly how much detail about the system should be publicised. We thank the AEC for publicising the auditor's reports, but reiterate that source code review and testing in advance still do not prove that the system functioned correctly on the day.

The AEC kindly provided a demonstration of both systems, and we thank them for an interesting and detailed discussion. The rest of this submission details our recommendations for the current systems.

Computers in the ballot box

The system trialled at the last election was a good design for visually impaired voters. We support the extension of this scheme to other voters who have trouble voting by the usual paper-and-pen method. Our two main recommendations are:

- If the system is extended to voters who could remove their own printout from the printer and put it in the declaration envelope without help, it should include the option of a human-readable printout (which could have a barcode as well).
- For integrity checking on behalf of those voters who cannot put their own printout in an envelope, there should be regular, public checking of the barcoded output throughout the voting period, to ensure and demonstrate that the machine is recording votes correctly. We originally suggested that this check would not have to be done immediately, but could be done after the close of polls, possibly at the same time as the decoding of other declaration votes. However, the AEC has pointed out an important practical objection to this, being that if a problem was detected it would be too late to address the issue, and possibly (if the other affected votes had already been separated from their envelopes) too late to identify which votes came from the affected machine. It would certainly be possible to do this check throughout the day (or at the end of the day) at the polling stations, though this would involve the extra cost (and the extra privacy risk) of placing the barcode readers in polling places. Perhaps some compromise is appropriate, in which the tests are decoded after polling but before the other declaration envelopes are opened. Then, though it would be too late to give affected voters the opportunity to revote, it would still be possible to identify the suspect votes and remove them from the system. It is important to realise that this check would, in the overwhelming majority of cases, result in 100% correctness. (After all, the argument given in the last election was that such a check was unnecessary because the computers were perfectly trustworthy.) It would serve as immediate evidence of the system's correct functioning, and a check against occasional (probably rare) faults.

Networked remote voting

Everywhere that it has been used, Internet voting has been criticised for its lack of transparency and accountability. Although Internet voting is still being used in some small and emerging democracies, and in Switzerland and Estonia, most advanced democracies that have trialled Internet voting have abandoned it. The United States' SERVE project, which was specifically for military personnel, was cancelled before deployment on the recommendation of the security experts commissioned to evaluate it [1]. (Though the Democrats Abroad voted by Internet in the last US election, and US election administrators could decide to conduct further Internet voting trials.) The government of the United Kingdom recently declared that there were no plans to run further trials of Internet voting, stating "Serious concerns persist about the security and transparency of e-voting systems and their vulnerability to organised fraud." [2] A French trial of Internet voting for overseas French citizens was widely criticised [3], and its future is uncertain. The concerns about security and transparency of electronic voting expressed by experts overseas apply in Australia too.

Running the system on the Defence Restricted Network (DRN) does not automatically solve these issues. It certainly does not solve the issue of transparency and accountability, namely providing evidence that the votes printed out by the system genuinely reflect the intentions of the voters. It is inappropriate for the legislation to treat these printouts as equivalent to real ballots – they are not, because there is a gap between the voter and the printout in which a malicious hacker, an accidental program error or a hardware fault could produce an incorrect result. There is no evidence of vote privacy that is nearly as convincing as the postal voter's chance to put their own vote in their double envelope.

We understand that there is a large group of voters who are, most unfortunately, disenfranchised by communications problems. We agree that it is important to address their needs, but don't believe that remote electronic voting is justified before the security and accountability problems are solved. We suggest considering alternative ways of using the communications infrastructure of the Internet (or the DRN) without necessarily trusting it. Some possibilities worth considering are:

- Perhaps ballot materials could be delivered via the electronic network, then printed out by voters and mailed to the AEC as postal ballots. Of course, this introduces its own security issues, particularly the oversupply of ballot papers, which are otherwise very carefully controlled.
- Perhaps the DRN could be used to establish a variant of mobile polling stations in which the computer running the voting application was placed in a proper ballot box and supplied with a printer. The votes could be sent back to the AEC over the network as they were in the recent trial, but afterwards the paper trail could be produced and mailed in a batch for verification.

We are not advocating either of these strongly, simply pointing out that there may be ways to use the communication advantages of an electronic network while preserving security and accountability. A similar proposal is included in the SERVE security report [1].

References

1. D. Jefferson, A. Rubin, B. Simons and D. Wagner, 2007. SERVE security report, www.servesecurityreport.org
2. J. Oates, 27th Oct 2008 "UK confirms e-voting death: no plans, no more trials," *The Register* http://www.theregister.co.uk/2008/10/27/evote_counted_out/
3. A. Appel, 2006, "*Ceci n'est pas une urne*," http://www.cs.princeton.edu/~appel/papers/urne.pdf

Declaration

The author's husband was an independent candidate for the Senate in the last election.