RECEIVED 28·5·10

COmputing
Research
& Education

Submission to the parliamentary inquiry into the functions and administration of voting centres

This submission examines the security and transparency of polling-place electronic voting machines. We believe that electronic voting should be as transparent as paper-based voting, and we explain why this is not currently so. We also discuss ways in which this could be achieved.

This submission is very similar to CORE's submission to the inquiry into the 2006 Victorian state election (submission 26), and our later submission to the inquiry into voter participation and informal voting (submission 10). For this inquiry we focus on issues of transparency.

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 Tom Gedeon.

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.

Signed by Vanessa Teague:_____

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

Introduction

CORE has made several submissions about security and transparency of electronic voting. The fundamental point is that a computer may not necessarily record or transmit the vote that the voter wanted. This may be because of accidental software or hardware errors, malicious tampering by outside hackers, infection by viruses, trojan horses or other malware, or even manipulation by insiders. The system should be designed so that its correct behaviour is transparently observable, by voters and scrutineers, so they do not have to trust that the computer is behaving as expected. Our previous submissions [1,2] made three main recommendations:

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).**

In this submission we will focus on points 1 and 2, which concern the transparency of the electronic recording and counting of votes.

1. Verifiable Voting

Our first recommendation was that the system should provide a voter-verifiable paper audit trail or "some other form of direct verification." Here we expand upon what is and is not a "form of direct verification." The objectives should be that

A. each voter gets good evidence that their vote was recorded as they intended, and
B. the scrutineers get good evidence that every vote was correctly counted.

That is, **the computerised system should achieve the same degree of transparency as the paper-based system we already have, without having to trust that the machines are working correctly.** Some examples are given below.

Examples of transparent (verifiable) voting:

i. *Printing a voter-verifiable paper trail, described in previous submissions [1,2].*

ii. *Using the computer to print a ballot [1,2].*

This is sometimes called an "electronic ballot marker." The printout would look and function just like an ordinary paper ballot. Able voters could check the printout and put it in the ballot box. Voters who were not able to read a printout, or not able to move it into the ballot box, should be able to instruct that this be done automatically (perhaps via a translucent chute from the booth to the ballot box).

iii. *Using a barcode printout, like the EVACS system deployed in the recent federal election, but augmented with the option of a human-readable printout.*

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

The EVACS system prints out a barcode which describes the vote but is not readable by a human. If each voter was given the option of also printing out a human-readable ballot on the same piece of paper, then this would provide a good check that the machine was behaving as expected. There could be procedures for scrutineers to verify that the human-readable printouts matched the corresponding barcodes. Voters who were unable to pick up and read their own ballot, or uninterested in verifying its correctness, could simply accept the barcode without making a human-readable printout. If a sufficient number of people printed and checked their human-readable vote, one could be confident that the rest of the barcodes were also correct.

iv. *Cryptographic schemes for end-to-end verifiable voting, as described in our previous submissions [1,2].*

The idea of these is to provide each voter with not only a proof that their own vote was recorded correctly, but also a mathematical proof that the entire election was correctly tallied. Although these schemes are promising, there is currently no system for sale that meets the requirements for Victorian elections. This is the current focus of the author's research.

Each one of the above provides evidence to the voter of correct recording of the vote, and each one produces a piece of paper that can be included in the scrutineering process. By contrast, we list below some designs that seem to achieve verifiability but in fact do not. In each of the systems below, if the voting machine was infected with malicious code, then votes could be undetectably misrecorded or incorrectly tallied, and that could alter the outcome of the election.

Examples of non-transparent (unverifiable) voting

i. *The scheme used in the last Victorian election, in which ballots were recorded electronically and printed at the end of the day.*

Voters had no way to check that the vote printed out on their behalf actually corresponded to their wishes. This issue is described at length in CORE's previous submissions [1,2].

ii. *The EVACS scheme with only barcodes and no option for human-readable printouts.*

The voter has no way to check directly that the barcode reflects their intention. This is described in CORE's submission to the federal parliament's inquiry into the 2007 election [3].

iii. *The scheme proposed for use in the upcoming Victorian election.*

This scheme is commercial software produced by a private vendor, Scytl. The vendor's marketing literature claims that their schemes provide "voter verifiability" because they have two separate software modules, one for recording the vote and another for "verifying" its correctness. Although this redundancy is a good way of catching accidental errors or hardware faults affecting only one module, there are still many attacks that could affect both modules, particularly since they are installed on the same computer. There is no evidence available to the voter that either module, let alone both, has

correctly recorded the vote, and there is no opportunity for scrutineers to verify the counting process. A hacker who took over the machine could just as easily simulate both modules as one. An accidental error, such as switching the party affiliations of two candidates, could very easily be repeated in both modules, since they are programmed, supplied and installed by the same people. Indeed, an expert review [4] of another Scytl system, deployed by the State of Florida, USA, found that "the software architecture alone does not address many insider threats," and that "the system does not provide the counted-as-cast property," "if malware were introduced onto the voting kiosk, it could violate the requirements for a secure election," and "malicious insiders may be able to attribute votes to voters." Scytl claims to have addressed many of these issues, but it is impossible to evaluate the extent to which they have succeeded, because their source code remains secret.

2. Source Code Transparency

For the upcoming election, the Victorian Electoral Commission has encouraged the vendor (Scytl) to release some details of their system to CORE for analysis. Although Scytl consented in principle to releasing some source code, they insisted on some form of non-disclosure agreement. The author is currently negotiating with Scytl for some degree of access to some information. At the time of writing, no agreement has been reached and Scytl has not released any detailed information about the system being deployed.

We question whether it is appropriate for the Victorian election to depend on the correctness of a software system whose details the VEC can not release to local experts for analysis even when they would like to.

Summary

Transparency is a vital part of the electoral process. Whether voters use computers or a pencil and paper to express their vote, they should get good evidence that their vote is cast as they intend, and the scrutineers should get good evidence that all votes are counted correctly. Neither is true of the current e-voting system in Victoria. We have suggested several alternative designs for secure, transparent electronic voting.

References

1. Computing Research and Education Association of Australasia (CORE), submission to the Victorian Parliament's inquiry into the 2006 Victorian State Election (submission 26),
2. Computing Research and Education Association of Australasia (CORE), submission into the Victorian Parliament's inquiry into voter participation and informal voting (submission 10).
3. Computing Research and Education Association of Australasia (CORE), submission to the inquiry into the 2007 federal election (Submission 116).
4. M. Clarkson, B. Hay, M. Inge, A. Shelat, D. Wagner and A. Yasinac, "Software Review and Security Analysis of Scytl Remote Voting Software," September 19, 2008. Report commissioned by the Florida Division of Elections. www.cs.berkeley.edu/~daw/papers