EMC Submission No 22
Received 3 July 2015

SUBMISSION TO VICTORIAN EMC INQUIRY INTO THE CONDUCT OF THE 2014 VICTORIAN STATE ELECTION

Vanessa Teague,
Senior Lecturer,
Department of Computing and Information Systems,
University of Melbourne
[redacted]

Rajeev Goré,
Professor,
Research School of Computer Science,
ANU, Canberra.
[redacted]

This submission repeats the main points of our prior submissions to the Victorian and other Australian parliaments, updated with some extra detail on electronic voting and counting in Victoria and other states and territories.

We would be happy to discuss or expand upon these issues, or any issues raised in the previous submissions.

We are endorsed by the executive of CORE as Experts for the purposes of this submission. The Computing Research and Education Association of Australasia, CORE, is an association of university departments of computer science in Australia and New Zealand.

Teague worked (on a voluntary basis) with the Victorian Electoral Commission on their e-voting project based on Prêt à Voter. With colleagues she has published several academic papers on the subject.

She is proud to be on the advisory board of Verified Voting. Concluded advisory roles include the University of Luxembourg's Secure and Trustworthy Voting Systems project and the University of Surrey's Trustworthy Voting Systems Project. She recently departed the advisory council of the US Overseas Vote Foundation's end-to-end verifiable Internet Voting project. She is an editorial board member of of the USENIX Journal of Election Technologies and Systems, and a program committee member of various cryptography and electronic voting conferences including EVOTE ('15), Vote-ID, RSA-cryptographers' track ('14 and '15), Applied Cryptography and Network Security ('15), and the European Symposium on Research in Computer Security ('15).

She receives funding only from The University of Melbourne and the Australian Research Council (apart from occasional one-off travel reimbursements *etc.*), including a current grant on electronic voting privacy.

Goré is an expert in formal methods applied to vote-counting programs for complex counting schemes such as single transferable voting as used in Victoria. He is on the programming committee of the 2015 Vote-ID conference to be held in Bern in September.

Goré currently holds a DP14 grant on electronic vote-counting and the project aims to produce formally verified vote-counting programs for use in Australian elections.

Goré and Teague, with other colleagues, have applied for a DP16 grant from the Australian Research Council to explore methods of improving electronic voting and counting in Australian elections.

We are scheduled to give a seminar on our research at the Parliament House library in November 2015.

INTRODUCTION: TRANSPARENCY AND VERIFIABILITY IN E-VOTING

Achieving transparency and verifiability in computerised voting is very difficult, because a person cannot observe directly what a computer is actually doing. A voter interacting with a PC, or a group of scrutineers watching a display screen, cannot actually observe what is happening to the electronic data. Hardware and software errors, accidental configuration errors, or deliberate manipulation or hacking, could all cause privacy to be breached or votes to be modified, misrecorded or dropped. A brief look at a week's technical news shows that electronic security breaches on important government and financial infrastructure are common. For example, this month Chinese hackers were blamed for a serious breach of the US office of personnel management, which held data on US federal employees including those seeking security clearances[1]. Electronic voting systems would not be immune.

Transparency, privacy and verifiability have been fundamental requirements of Australian electoral administration since long before computers were involved. Much of the current nationwide debate on voting technology centres on how to adapt these principles to computerised elections. There are two important themes:

*1. **Transparency**, in form of the system's source code and documentation being publicly available for open review.*

*2. **Verifiability**, in the sense that for each election, each voter should get good evidence that their vote is cast in the way that they intended, and scrutineers and the public should get good evidence that all the votes are properly input and accurately tallied.*

Teague has been working with the VEC on a voluntary basis on their current project based on Prêt à Voter and has coauthored several academic papers on the subject. This scheme provides verifiability of all steps in the voting and electronic delivery process, and all the source code and documentation are publicly available. This should allow electronic voting to become part of the ordinary process of scrutiny, review and improvement that is a vital part of electoral administration.

Like any leading-edge project there were important new insights from the first run that need to be addressed next time. These are outlined below after a summary of verifiability and transparency for e-voting.

VERIFIABILITY

***Recommendation (from 2011 sub):** For each election, each voter should get good evidence that their vote is cast in the way that they intended, and scrutineers and the public should get good evidence that all the votes are properly input and accurately tallied. 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.*

The idea of verifiability applies to all elections, not just electronic ones. Unlike elections conducted in a single attendance polling place and based on paper, electronic processes are inherently opaque to observers, so even a group of scrutineers standing around the computer cannot actually verify directly that it is doing the right thing to the ballot data. Nor can a voter using a computer verify directly that the computer is writing the electronic vote that the voter wanted.

---

1 http://www.theguardian.com/technology/2015/jun/04/us-government-massive-data-breach-employee-records-security-clearances

“Verifiability” needs to be made precise in order to be meaningful. Indeed, many electronic voting software vendors advertise “verifiable” products which in fact provide very little meaningful evidence of having recorded, collected or counted the votes correctly.

“Voter verifiability” (sometimes called cast-as-intended verifiability) is the first step – this is where a voter gets evidence that their vote is cast as they intended it WITHOUT HAVING TO TRUST THE COMPUTE CODE THAT IS USED TO CAST THE VOTE. A verifiable election also needs to show that the vote was properly dealt with after that. It should be possible for voters and observers to verify that all the votes were counted as the voter cast them, and then correctly tallied. Systems with all three kinds of verifiability are called “end-to-end” verifiable because every step of the process is verifiable. The VEC's vVote project is based on Prêt à voter, an end-to-end verifiable voting scheme.

A simple way to achieve cast-as-intended verifiability for electronic voting is to augment computer-assisted attendance voting with a human-readable paper trail. This simple and verifiable solution is offered in Tasmania and WA to voters who have difficulty using paper and pencil. The voter interacts with a computer, which then prints out their vote for insertion into an ordinary ballot box alongside all the other votes. This allows each voter to verify that the printout matches their intentions, then scrutineers observe the counting process just as they observe all the other paper ballots being counted.

ATTENDANCE END-TO-END VERIFIABLE ELECTRONIC VOTING: THE EXAMPLE OF VVOTE

Vvote is the VEC’s end-to-end verifiable attendance voting project, based on Prêt à Voter. The cryptographic component was produced by an international team led by the University of Surrey and including Luxembourg and Melbourne. Voters have the opportunity to verify that their votes are cast in the way that they intended, and properly included in the count, and the system produces a public mathematical proof that all the votes (from this system) are accurately output. This project is particularly well suited to early and absent *attendance* voting, because it provides verifiability without dependence on a secured trail of paper votes.

vVote provides a high degree of privacy and verifiability, but also requires substantial investment of money, time and effort in order to achieve the integrity properties it is designed to achieve. The code will need continued maintenance and development as bugs are found and modifications are implemented. Polling place procedures include complicated steps for setting up the polling place, protecting voters' privacy, and for allowing voters to verify that their Prêt à Voter ballot is properly constructed so that their vote will match their intention. These steps must be followed, and voters must be educated about them, in order to achieve the integrity properties of the design. Teague wrote an outside guide to verification aimed at voters in the 2014 election (http://electionwatch.edu.au/victoria-2014/click-here-democracy-e-vote-explained), but these sorts of instructions need to be part of the ordinary voting process, easily accessible to all voters, in order for the system to achieve its objectives fully.

A similar observation applies to privacy: an important step in preserving vote privacy is to shred the candidate list after voting. Without this step, the retained candidate list represents a risk to vote privacy. Overall numbers are also important – there must be a large enough number of voters in each division to provide anonymity.

The advantage of vVote is that electronic votes can be transferred with verifiable evidence of their correctness, without relying on the security of a paper trail. This is particularly advantageous for overseas polling places. However, the VEC may decide that the difficulty of implementing the pollsite verification procedures outweighs these advantages, in which case they could easily reuse their existing open-source user interface to produce an ordinary human-readable paper trail.

REMOTE ELECTRONIC VOTING: THE EXAMPLE OF IVOTE

Secure and usable remote electronic voting, *i.e.* Internet voting, remains an unsolved problem, and we have argued in the past that the risks outweigh the perceived benefits. There are various software products available that purport to provide security and verifiability, but experience in other states, particularly NSW, has shown serious problems relating to reliability, privacy, security and verifiability. The general issues are described in our prior submissions. We won't repeat them here, but instead concentrate on the lessons derivable from Teague's analysis with Alex Halderman of the security of the NSW iVote Internet voting system. iVote was implemented by Scytl and run in the recent NSW State Election.

The abstract of the paper is included here. The full analysis is available at http://arxiv.org/abs/1504.05646

> *In the world's largest-ever deployment of online voting, the iVote Internet voting system was trusted for the return of 280,000 ballots in the 2015 state election in New South Wales, Australia. During the election, we performed an independent security analysis of parts of the live iVote system and uncovered severe vulnerabilities that could be leveraged to manipulate votes, violate ballot privacy, and subvert the verification mechanism. These vulnerabilities do not seem to have been detected by the election authorities before we disclosed them, despite a pre-election security review and despite the system having run in a live state election for five days. One vulnerability, the result of including analytics software from an insecure external server, exposed some votes to complete compromise of privacy and integrity. At least one parliamentary seat was decided by a margin much smaller than the number of votes taken while the system was vulnerable. We also found protocol flaws, including vote verification that was itself susceptible to manipulation. This incident underscores the difficulty of conducting secure elections online and carries lessons for voters, election officials, and the e-voting research community.*

Approximately 66,000 votes were cast in the days before the security problem was identified and fixed.

Some first-preference NSW Legislative Council vote tallies produced by iVote differed notably from those received via paper-based methods. For example, the ALP received more than 30% of the vote from every other method, but only 25% of iVotes[2]. The reason for this discrepancy is unclear. We know of no way to discern whether this was a result of a donkey vote (whatever that means), a user interface problem, a software error, or a security breach involving deliberate vote manipulation.

Publicly available information about iVote is very limited, with no source code and only vague overviews of the system's structure available. There is some opportunity for voters to query a verification system and check that their vote was recorded as they intended, but only a very poorly-described process for a limited number of participants to verify the subsequent vote processing.

At present no Internet voting solution exists that provides a degree of security and verifiability as good as postal voting for those who can fill in their own postal vote. For voters who need assistance filling in their own paper vote, the two verifiable attendance electronic voting solutions mentioned above provide superior security and verifiability to any Internet voting solution now available, or likely to be available in the near future. Disabled voters' democratic rights are not improved by providing an accessible remote voting solution that does not protect the integrity or privacy of their vote as well as alternative methods.

---

2 http://blogs.abc.net.au/antonygreen/2015/04/does-electronic-voting-increase-the-donkey-vote.html

ELECTRONIC DELIVERY AND PAPER RETURNS

We have previously suggested electronic delivery of ballot information and paper (postal) voting returns, especially for local government elections which are otherwise a significant burden on the postal service. Although this remains subject to some of the same challenges as postal voting, it at least gives voters the opportunity to verify that they send the vote they intended to send. This might help in the administration of local government elections, or address some of the problems that seem to need Internet voting.

TRANSPARENCY

Recommendation (from 2011 sub): *As much as possible of the system's technical details (including source code) and documentation (including documentation on the development processes and reports on the audit and evaluation) must be available to scrutineers, security experts and the public. This level of transparency should be an enforced condition of the initial tender and contract.*

The VEC has chosen to make all vVote's source code and system details public.

ELECTRONIC COUNTING AND RANDOMISED CANDIDATE DRAW

Since the last election the VEC have also published the source code for their STV Legislative council count and their program for electronic randomised candidate draw. Below-the-line voting data is made easily available for research and double-checking of the count. All of these are to be applauded, though of course there should also be a process for securely reconciling the electronic legislative council vote data with the corresponding paper evidence.

One subtle but important issue is in the seeding of the random ballot drawing process. Like all electronic random processes, the computation must start with some random values input to the program from an outside seed. The source code itself doesn't give much of a clue about this, because it is simply a call to a function called `new Random()`, without enough context to understand what this does. In principle, even if the code itself was a valid (pseudo-)random ballot draw, a person with knowledge or control of this random seed could use it to direct the ballot draw to a desired outcome — it could be as simple as running the program multiple times, with different random seed values, until a desired outcome was produced. (We are not in any way suggesting that the VEC currently do this. We are suggesting that they could easily improve their process to one that demonstrated publicly that it was impossible for anyone to do this, rather like the electronic equivalent of the spinning wooden box they used to use.)

The simple solution is to ensure that this initial random seed is derived in a public way from a genuinely random process, for example by throwing dice under observation by the candidates. The resulting random value would then serve as the seed for the electronic random process. This would then allow anyone to reuse the publicly available code for checking the computation of the candidate draw. A similar process is used in the USA for risk-limiting audits of paper ballots.

ELECTRONIC COUNTING: ANOTHER COMPARISON WITH NSW

For comparison, and to explain why all this transparency is important, consider the situation in the most recent NSW state election. The entire state of NSW consists of one electorate choosing 21 candidates for the Legislative Council, using a variant of the STV algorithm, in which a randomised process is used for distributing votes in excess of a quota when a candidate is seated. NSW voters may cast more than one preference either above or below the line. As in Victoria, NSW Legislative Council votes are counted electronically. Unlike Victoria, the source code for the NSW process is unavailable to the public.

In the recently-concluded NSW state election, the last seat in the Legislative Council came down to a very small margin, 3177 votes out of a total over 4 million. The Animal Justice Party narrowly won; the No Land Tax Party narrowly missed out. Before the final count, many commentators including Antony Green predicted[3] that the Animal Justice party would probably lose the seat and perhaps challenge the election result based on some administrative errors in iVote. After the count, the No Land Tax Party told the media they intended to challenge. The outcome depended crucially on preference flows, of which the Animal Justice Party received many and the No Land Tax Party very few, reversing the parties' order compared to first-preference tallies[4].

At the time of writing, more than 3 months after the election, voting data for second and later preferences remains unavailable to the public, despite those preferences having been crucial determinants of the outcome of that last seat. NSWEC has released only first-preference tallies and their own distribution-of-preferences count[5], refusing repeated requests from our colleagues, ourselves and others to provide the full preference data. This means that there is no opportunity for an independent assessment of whether the announced outcome of that last seat was correctly computed, what the true margin was, or with what probability different randomised preference distributions might have produced a different outcome. Nor is it possible to examine the iVote returns separately to understand whether security or other problems might have caused them to differ from the paper returns in a way that could have affected this outcome.

Of course, none of this proves that the announced outcome is wrong. However, well-run electoral processes should produce evidence that they are correct, not an absence of evidence either way.

In summary, NSW has a seat in the Legislative Council for which the election outcome is close (compared to both the overall election size and the magnitude of problems in the conduct of the election), disputed (at least informally), and surprising (to at least one informed commentator). There is not even enough publicly-available information to allow double-checking for accidental tabulation or counting errors, and no publicly available evidence that the seat has been assigned to the true winning candidate.

ELECTRONIC COUNTING: EXPERIENCES FROM THE ACT

Since 2001, the ACTEC has used an electronic vote counting program to count some of the votes cast in the elections held every four years. More recently they have extended it to count all votes. The code for vote-counting is available for public scrutiny from the ACTEC website.

Using the publicly available vote counting code, the ANU Logic and Computation Group have found three bugs in the code. The ACTEC have acknowledged and fixed all bugs. For each bug, it was possible to design an election scenario in which the bug would have led to an incorrect count.

Goré and colleagues have also written their own vote-counting code. They have checked that the final results for the past four elections are the same using our vote-counting code. Thus we are confident that none of the bugs have actually manifested themselves in the previous elections.

The ACTEC is to be congratulated for making their vote-counting code publicly available for scrutiny.

The VEC's recent decision to make their counting code available permits the same sort of analysis, which should have the same positive implications for reducing the number of bugs.

The ultimate aim should be replace all of this in-house code with formally verified code which is provably correct with respect to its specification. This is the topic of Goré's current DP14 grant.

---

3 http://blogs.abc.net.au/antonygreen/2015/04/legislative-council-count-updates.html

4 http://vtr.elections.nsw.gov.au/lc-home.htm#lc/state/fp_by_grp

5 http://vtr.elections.nsw.gov.au/lc-home.htm#lc/state/dop/dop_cnt_001

CONCLUSION

Enhancing access for voters with disabilities and decreasing accidental informal voting are both important benefits that come from electronically assisted voting. It's important that these benefits come with a continued emphasis on verifiable election outcomes and transparent electoral processes.

In general anything that uses technology for improved communication with voters is probably an improvement; technology that is used as a trusted medium for taking and transferring votes needs to be approached with great caution, and subject to the extensive scrutiny and verification applied to other processes that take and transfer votes.

Teague has supported and worked (on a voluntary basis) on the VEC's vVote project over the last few years. The project has gained significant international attention as the first run of end-to-end verifiable voting in the world at a state election level. The lessons learnt from the 2014 run, particularly the complexities involved in implementing the right polling place procedures, will hopefully be turned into an improved deployment next time. Of course, technology moves fast and is likely to undergo changes over the next few decades. The VEC may also decide to fall back to a simpler system with a human-readable paper trail. What's most important is that the right culture and structures are put in place so that it will continually improve, in the same way that paper-based elections do. Transparency, verifiabililty, in-house expertise and scrutiny are necessary components of this.

We believe that both the Victorian EMC and their federal counterpart have made the right decision in not permitting Internet voting, and that the recent iVote run reinforces this decision.