Submission No 36

2012 LOCAL GOVERNMENT ELECTIONS

Organisation: Computing Research and Education Association of Australasia

Name: Dr Vanessa Teague

Date Received: 8/02/2013

NSW EMC

SUBMISSION TO THE NSW JSCEM INQUIRY INTO 2012 LOCAL GOVERNMENT ELECTIONS

DR VANESSA TEAGUE AND DR ROLAND WEN

7TH FEB 2013

CORE is an association of university departments of computer science in Australia and New Zealand. The authors are both Computer Science and Engineering researchers whose main interest is in electronic voting and security. Vanessa Teague is a research fellow in the department of computer science and software engineering at the University of Melbourne, with a research emphasis on secure electronic voting. Roland Wen is a research fellow in the School of Computer Science and Engineering at the University of New South Wales, and in the Department of Computing at Macquarie University. His research focus is security and engineering practices in electronic elections. This report has been endorsed by the executive committee of CORE.

We would be very happy to discuss electronic voting further with the committee. Vanessa Teague can be reached by email at vjteague@unimelb.edu.au, or by phone at (03) 8344 1274. Roland Wen can be reached at rolandw@cse.unsw.edu.au.

USE OF INTERNET VOTING IN LOCAL GOVERNMENT ELECTIONS

The reasons for not currently adopting Internet voting for local government elections are the exact same as those for not using it in State elections, as described in our submission to the JSCEM's previous inquiry into the administration of the 2011 State election. The issues include verification of the accuracy of the result, privacy of individual votes, authentication of eligible voters, and transparency of the electoral process.

The NSWEC has undertaken to address all of these issues in the future, but the authors believe that this could well be impossible, as detailed below in this submission.

Here we discuss a set of technical requirements and characteristics relating to a software system. Accordingly, the first parts of this submission (on verification and privacy) consist of a set of technical questions related to the next version of iVote. The last section (on transparency) questions how the necessary answers will be found to these outstanding technical questions.

VERIFICATION

Everyone agrees that election outcomes should be verifiable, but the JSCEM's report on the 2011 state election only partially addresses this issue:

4.87 To this end, the Committee is pleased to note the NSWEC's recommendation that iVote should provide voter preference verification (in such a way as to not reduce the secrecy of the voters' ballot) and this recommendation is supported. (Parliament of New South Wales, Electoral Matters Committee, 2012)

"Verification" needs to be more clearly defined here. In our submission to the previous inquiry we recommended that the system "provide evidence to voters that their votes are cast as they intended and properly included, and evidence to scrutineers and observers that all votes are properly printed or properly electronically tallied." The NSWEC's proposal to provide "voter preference verification" addresses just one of these three steps: that a voter gets evidence that their vote is cast (at their PC) in the way they intended. This raises several technical questions:

1. What evidence is provided that the votes are printed (or electronically tallied) in a way that matches the value the voter has verified? (In other words, what prevents or detects manipulation after the "preference verification"?)
2. Who sees this evidence? The voter themselves, the public, the scrutineers, or a single auditor?
3. What are the situations in which the "preference verifications" succeed but the electronic vote data is nevertheless manipulated?

PRIVACY

The clause about not reducing the secrecy of the voter's ballot is also crucial. "Reducing" is a relative word. Will it be "not … reduced" relative to the existing iVote architecture in which anyone with administrator privileges on the server can link every iVote ID to its (unencrypted) vote? Or relative to the situation of vision impaired voters who have to tell another person their vote if they use paper? Or relative to the situation for postal voting or early voting?

4. Does the proposed preference verification step allow an auditor to match the voter's iVote ID with their vote?

5. Does the proposed preference verification data allow an auditor to infer the votes of those who have not verified?
6. Is it possible for an auditor to infer the identity of the voter from their iVote number or other information collected during the preference verification?

TRANSPARENCY

We encourage the JSCEM to rethink their recommendation on transparency:

4.89 On the issue of transparency, the Committee notes differing stakeholder views as to the best way to evaluate electronic voting systems, whether it be via expert review under non-disclosure agreements as favoured by the NSWEC or open review through unlimited access to the source code such as that being developed for vVote. (Parliament of New South Wales, Electoral Matters Committee, 2012).

Our recommendation of openness of the source code and documentation is not a "stakeholder view". Transparency of election systems has been a universal principle since long before computers were involved. A transparent system, whether electronic or paper-based, gives all stakeholders evidence about whether the votes are kept private and properly dealt with. It allows for an open process of accurate evaluation and improvement. A private audit under NDA would not be an adequate substitute for open scrutineering of paper-based voting. Similarly, a private audit under NDA will not provide good evidence that the software system protects privacy or provides verifiability in the way that it is advertised. Even a diligent, motivated and expert auditor could miss vulnerabilities.

Making a system open source does ***not*** automatically make it secure. We said this clearly to both the NSW JSCEM and the Victorian EMC. However, keeping its source code secret apart from NSWEC-appointed "experts" under NDA makes it highly unlikely that an accurate assessment of its vulnerabilities will be published in time to affect decisions on its use, let alone in time for addressing those vulnerabilities prior to the election. Having the open source available to the community for technical review by a range of interested experts will both increase transparency of the electronic voting process, as well as enable a wider range of expertise to be deployed.

The reason this issue is so contentious is that the business interests of the software vendor differ from the transparency requirements of election administration. A vendor's priority is its commercial interest. Its obligations are to protect the value of the IP related to its product and also the value of its reputation (obviously it's bad for business if failures, vulnerabilities and shortcomings come to light). This is largely achieved through legal instruments such as NDAs.

This makes it difficult for an electoral commission with obligations to protect election integrity and provide the strongest support for transparency and scrutiny. We have recommended elsewhere that strong requirements for openness be part of the initial tender and contract, so that the electoral commission retains ownership and control of the electoral process. An early feasibility study for the iVote project also recommended,

"The electronic system, then, needs to be provided to the public in a way that matches the openness of the paper system. Indeed, this open approach has already led to better electronic voting schemes:-"Experts and all other interested parties are in fact encouraged to evaluate and criticise the scheme. The intent is to expose any flaws or weaknesses, and subsequently work towards improving the scheme." " (Nesci & Burton, 2009)

Powerpoint slides simply do not provide enough technical detail to allow observers to understand how the system works, or be confident that it achieves what it is supposed to do.

Experience in Australia demonstrates the clear advantages of openness. The publication of the ACT EVACS source code enabled two independent groups of experts to analyse the e-voting system. This revealed problems that evaded detection in private audits, and some were fixed for subsequent elections (Gore). Similarly, my reading of a detailed protocol-level description of the VEC's 2010 system allowed me to identify a vulnerability in time for the vendors to patch it (Teague, 2011).

An open-source system is not necessarily more expensive than a proprietary one of similar quality and functionality. For example, the Norwegian Internet voting project did indeed cost approximately ten times as much as iVote. However, the project price included a new electoral management and "e-counting" systems, and the Norwegian authorities now own all IP rights to the software, with perpetual licenses on the vendor's patents.

A critical question to ask is if a non-disclosure agreement is required, who is going to provide accurate and reliable answers to the technical questions above? For example, take the central question of the verification protocol:

> *What are the situations in which the auditor's checks succeed but the electronic vote data is nevertheless manipulated?*

We appreciate this is what's not supposed to happen. The question is, who demonstrates that the verification protocol is not buggy? The verification protocol advertised in the last state election as "confirm[ing] there has been no tampering to the vote," (NSWEC, 2011) is now agreed by all parties to have proved nothing of the kind. If we hadn't pointed this out, how would the JSCEM now know? Did the private security firm working under NDA notice that problem last time? If a private security firm under NDA again evaluates the new verification procedure, how can we be confident that the new one isn't buggy too?

The same thing goes for privacy. It seems highly unlikely, based on our experience of other systems, that an architecture without client-side encryption could allow for preference verification without revealing the vote to a third party (such as an auditor). Who is going to evaluate accurately whether this is true?

The notion of "expert review under NDA" begs the question of who the "expert" is going to be. We have already recommended complete openness of all of the system's technical details including source code and other documentation. This means that extensive review by a wide variety of people is possible. Furthermore any vulnerabilities or shortcomings can be clearly and publicly demonstrated, or refuted using logic and evidence, without recourse to ad hominem about who is a "self-styled expert" and who isn't.

We respectfully suggest that publishing auditors' reports and other technical data after the 2015 state election (NSWEC, Response to Submissions, 2012) is not an effective method of discovering and patching vulnerabilities before the election. Nor is it an effective method of allowing voters to make an informed decision about whether to trust the system or choose a different method of voting.

A FINAL COMMENT ABOUT ACCESS

Vision impaired voters have the right to a private and verifiable independent vote. The iVote system fails to protect this right. Many of the advertisements that have made the system popular are not accurate. Depending on a computer is not a form of "independence", it's a different dependence. Vision impaired voters should have the option of choosing for themselves given accurate technical information in advance of the election.

We query the claim that iVote provided greater access for other classes of electors.

(NSWEC, Response to Submissions, 2012): *"Also, iVote provides greater access to the electoral process for several classes of elector. In particular at the last general election it was noted that there were an additional 20,000 interstate and overseas voters who voted using iVote. In past elections these electors could not vote using traditional voting channels."*

First, there are other voting channels for many eligible iVote users, including postal voting and pre-poll attendance voting. Second, there was no way for the NSWEC to check for sure who was actually overseas or interstate[1]. A person could easily have claimed to be away from the state on polling day when they weren't. Thus the claim that iVote provided for "an additional 20,000 … voters" is not well justified.

CONCLUSION

The JSCEM has recommended voter preference verification without insisting on verification of the rest of the process. Although the NSWEC has offered to ensure the changes "not reduce the secrecy of the voters' ballot" this clause is omitted from the JSCEM recommendation. Both these requirements, verification of the post-voter-verification step and protection of vote privacy, should be present, for the same reason they are expected of other methods of voting.

An evaluation process by NSWEC appointed "experts" under NDA did not detect a range of serious problems related to reliability, verifiability and privacy of iVote last time. A transparent public process including publicly available source code and documentation would be much more likely to produce an accurate evaluation.

BIBLIOGRAPHY

Gore, R. (n.d.). manuscript.

Nesci, & Burton. (2009). *Alternative Voting Methods for Vision Impaired Electors.* Commissioned by NSWEC.

NSWEC. (2011). *iVote Approved Procedures for 2011 NSW State General Election.*

NSWEC. (2012) *NSWEC and Election Funding Authority Responses to submissions to the inquiry into the administration of the 2011 NSW election and related matters.*

Parliament of New South Wales, Electoral Matters Committee. (2012). *Administration of the 2011 NSW Election and related matters (Final Report).* Sydney.

Teague, V. (2011). *CORE Submission to the Inquiry into the 2010 Victorian State Election.*

[1] One can tell from the IP address the domain of the source computer, which gives significant clues about its location. However, this would probably not allow for confidently distinguishing different Australian states, and could be easily subverted even for those claiming to be overseas. For example, someone with an account on an overseas computer could use it to vote after logging in remotely from within NSW.