CORE

Computing Research & Education

CORE Submission to the Inquiry into the 2010 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 Vanessa Teague and Roland Wen 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. Roland Wen has recently submitted his PhD thesis at UNSW on secure online elections in Australia.

We would be very happy to discuss any of these issues further.

Summary

This submission is an attempt to give an overview of the options for using computers to assist in the voting process. For each solution, we discuss the extent to which the solutions could achieve reasonable privacy, transparency and security. We also comment upon some recent electronic voting trials in NSW and Victoria, using only information that is publicly available.

Introduction

Australia has a long history of transparent, professionally-organised, secret ballot voting. If Australia moves towards electronic voting, it is crucial that the uncompromising quality of our elections is maintained. The principles of privacy, integrity, transparency and scrutiny that apply to paper-based voting in Australia should apply just as strongly to electronic voting.

Two kinds criticisms apply to electronic voting. One is a non-technical criticism of the processes employed in particular trials; the other is a rigorous technical analysis of the security properties of the technologies available.

The processes

If we do consider electronic voting, whether consisting of computers in polling stations or remote Internet voting, then privacy, integrity and transparency should be central to the discussion from the beginning. There is no more reason for a secret, unscrutinised electronic voting process than there is for any other secret process that injects votes into the tally without adequate scrutiny. Scrutiny improves security because it allows problems to be identified and rectified. As we wrote in our 2007 submission, it is a common fallacy that secrecy makes electronic systems more secure.

Recommendation 1: Computerised voting systems, including their source code, all documentation and reports, and the associated physical security procedures should be available to e-voting and security experts and the public.

The recent trend at both state and federal level to entrust electronic voting to secretive private vendors is not consistent with the degree of transparency we expect for Australian elections. Whether the integrity or privacy of the systems meets our expectations is unclear because we have no details about them. For example the NSW iVote project has been carried out in a clandestine manner. Neither the iVote system nor any associated documentation has been made available for scrutiny by e-voting experts and the public. The NSW Electoral Commission intends to release only the auditor's final report, but on its own this will provide little if any evidence of iVote's security. The Victorian Electoral Commission's electronically assisted voting project had a higher standard of transparency, allowing Dr Teague to read enough information to make some constructive comments about the security of the system (Teague, (CORE, 2010)). Even so, there were some issues that were impossible to analyse without source code.

The technologies

Computers are just machines executing programs written by people. Just because a vote is cast on a computer does not necessarily mean that the vote is recorded or transmitted correctly, or that it remains private. Computers may have unintentional program errors (bugs), or they may have security vulnerabilities that allow malware (viruses, worms, or Trojan horses) or hackers to take control. Any of these could cause a vote to be cast that did not reflect the voters' intention, was not properly transmitted, or was not correctly counted. They could also compromise vote privacy.

Some Australians experience difficulty using the traditional pencil and paper method of voting. People who cannot write their own ballot have traditionally had to depend on another person, who obviously learns their vote. People who cannot see their own ballot have generally had to reveal their vote to another person and also depend on that person to express the vote they asked for. It is entirely understandable to want to address this problem, but we emphasise that just because a vote is cast on a computer does not necessarily imply that it is cast correctly or that its privacy is preserved.

No system, whether based on computers or paper, is perfectly secure or provides absolute privacy. When considering different voting options, we should consider whether the security properties of the new solution actually improve upon the system it is replacing. It is important to realise that the security and privacy of the systems currently available to visually impaired voters are far below the guarantees provided to sighted voters. Consequently a system that represents an improvement for visually impaired voters might be a serious step backwards for sighted voters. The best options for visually impaired voters may be completely different from those of Antarctic or outback voters.

Recommendation 2: It should be recognised that the systems designed to address the unique usability and integrity concerns of visually impaired voters are not necessarily appropriate solutions for others.

Specific issues

We give an overview of the specific technical issues relevant to electronic voting. Each of them will be revisited when we consider particular kinds of electronic voting below.

1. **Vote verifiability:** The most important issue in computerised voting, and one which arises also for people who have to trust others to vote on their behalf, is the question of whether the vote cast actually expresses the intention of the voter. Sighted Australians who fill in their own paper ballot don't need to consider this problem, because they can see clearly what numbers are filled in on their own ballot.[1] Voters who entrust the recording of the vote to a person or computer should ask what guarantees they receive that the vote is being recorded as they intended. This issue of whether the voter can verify that their vote is cast as they intended will be a major theme of this submission.

   Allowing voters to verify that their vote is cast as they intended is straightforward for sighted voters using a computer at a polling place – simply make the computer print out a human-readable vote that the person can check and then hand to the polling officials. The problem is much more difficult for visually impaired voters and for voters over the Internet. Although some research exists on both these issues, neither is a solved problem. Some work on the latter is described below.

2. **Privacy** remains a serious issue when an electronic record of the vote is maintained. It is a common misconception that computers guarantee privacy automatically. Some privacy issues are easier to address electronically than by post, such as the problem of making a message difficult to intercept in transit. In other cases computerising voting makes the problem harder, such as the possibility that the computer may retain information about the vote in a way not possible for postal voting.

[1] They have to be careful not to disenfranchise themselves accidentally by skipping or repeating numbers, especially if they vote below the line. This is certainly a problem for verifiability, and one that could actually be solved by the use of computers, but it affects a relatively small fraction of voters.

3. **Voter authentication** is a serious problem for any form of remote voting, and particularly so for Internet voting, because the possibilities for large-scale automated voting on someone else's behalf are greater than for any other form of voting.

4. **Demonstrating that the vote count is correct.** For paper voting, the process of allowing scrutineers to observe the paper count is well understood. It is more complicated for postal voting because of delays and other problems in the post. For electronic elections, this can to some extent be addressed by cryptographic techniques for electronic voting

There is a great deal of difference between the degree of security provided by supervised computers in a polling station, as opposed to voting via the Internet. These are discussed separately in the following two sections, which also include comments on the recent Victorian Electronically Assisted Voting project and the NSW iVote project, with comparisons against some overseas systems. There are also other reasonable ways to use computers to help in the voting process, without resorting to a system in which the computers are "black boxes" trusted for the integrity of the election. This is particularly relevant to Internet voting, so some suggestions are included in the Internet voting section.

Internet voting

Internet voting in general presents major challenges for privacy, integrity and transparency. Many eminent computer security experts believe that it is not possible to secure Internet voting to a degree acceptable for a public election. Some representative quotations: "We do not currently have the technology to make internet voting secure (and may never)." (Rivest, 2010), and ""It is not technologically feasible today to make Internet voting safe against attack." (Wagner, 2010). Internet voting is becoming more common for private elections such as those for professional organisations and company shareholders, but public elections for government demand a far greater degree of privacy, security, transparency and public scrutiny.

For these reasons we should also consider whether there are other ways of using computers or telecommunications that would facilitate voting without necessarily trusting the computer and the Internet**.** For example, in CORE's 2007 submission we suggested using the Internet to distribute ballot papers, or using Internet-connected kiosks in mobile polling stations that also produced a paper trail. Similar suggestions were made by Rivest and Wagner, cited above. We are not advocating any particular solution, merely pointing out that there may be ways of using the Internet other than full Internet-only voting.

Recommendation 3: We should consider alternative methods of using the communications infrastructure without necessarily trusting it alone to carry completed ballots.

At present Internet voting is only defensible for those voters who do not currently have the opportunity to check that their vote matches their intention, such as visually impaired voters or voters who are unable to use postal voting.

Recommendation 4: If Internet voting is introduced, it should be only with the clear public explanation that the privacy and integrity of the system are significantly below those of postal voting. It is a last resort with limited integrity guarantees, appropriate at best for those who do

not get high integrity or privacy guarantees with alternative systems. This does not include ordinary postal voters.

NSW introduced the iVote system for Internet voting in the recent state election. There are however serious security vulnerabilities with the iVote system itself, as well as deficiencies in the processes for developing iVote and evaluating its security. We discuss these as examples as we discuss the major challenges for Internet voting in general.

Major Challenges

Authentication

Ensuring that only eligible voters vote, and that each one votes only once, is difficult for any method of voting. It is difficult in the polling place, and even more difficult for postal ballots, to ensure that the person casting the vote is the person on the electoral roll, not some other person attempting to vote on their behalf. Although authentication is imperfect for polling-station voting, and quite weak for postal voting, it is still extremely important to authenticate voters carefully for Internet voting. The opportunity for large-scale automated fraud, in which a small number of people cast votes that appear to come from others, is much greater for Internet voting than even for postal voting. Such fraud could be very difficult to detect, it could be impossible to discover who had committed it, and it could be impossible to prosecute if it came from outside Australia.

The NSW iVote system used weak authentication comprising an 8 digit user ID number and a short 6 digit PIN. This very low standard is not even acceptable for Internet banking. Banks in Australia typically require longer (and hence stronger) passwords, and many already use security tokens. It is telling that at least one of the submissions to this inquiry advocating federal Internet voting cited the increased convenience of not having to find a witness, as would be required for postal voting (Kennedy, 2011). It is absurd to deploy a less secure voting channel than postal voting and encourage people to use it instead of postal voting by reducing the authentication requirements below what would normally be required for postal voting.

In comparison, Internet voting in Estonia uses the strongest form of voter authentication: each individual owns a smart card (and a smart card reader) which contains a private key for which the electoral authorities know the corresponding public key. This provides a technical solution with a high degree of security. It also allows the vote to be digitally signed, which makes it much more difficult to modify undetectably after casting. Although this method would obviously be expensive to roll out to the general population in Australia, it may be feasible to implement for small, specific voter groups who are targeted for Internet voting, such as visually impaired or Antarctic voters. This and other options for strong voter authentication must be considered in order to evaluate the appropriate trade-offs between different costs and different security guarantees.

Another issue is authentication of the voting server to the voters, *i.e.* protecting the voters from being misdirected to a bogus website and hence prevented from casting a real vote.

Privacy

Vote privacy is a very serious issue for remote Internet voting for several reasons.

1. The unsupervised environment means that it is difficult to prevent other people from observing the voter.

2. The computer used for voting generally usually learns what vote was cast. This means that security problems on the computer, or legitimate control of the computer by another person, could reveal the vote**.** This is extremely difficult to avoid in practice, except with systems that are very difficult to use. It is a very serious problem for vote privacy since many remote voters would have to vote on a computer controlled (either legitimately or not) by someone else.

3. The system must be designed to preserve voter privacy even if the electoral commission's systems are compromised. For example, the process at the electoral commission must be very carefully designed so as to separate the decrypted vote from information identifying the voter**.** This is possible but difficult.

There is no justification available to the public as to whether the NSW iVote system adequately protected vote privacy. The system used an ordinary “secure” webpage, so the vote was encrypted by the voter's computer only in an ephemeral way that was decrypted immediately upon reaching the server. As a result anyone who gained access (authorised or not) to the electoral commission's systems could potentially have discovered how every iVote user voted. This means that vote privacy was entirely dependent on electoral commission procedures for preventing a person’s iVote ID from being linked to their identity. Details on these procedures are not in the public domain and may never be disclosed, meaning that there is no publicly available evidence that vote privacy was preserved.

It is important to note that this vulnerability could have been countered with standard cryptographic techniques that are already employed by many Internet voting systems. Hence the iVote system clearly falls well short of providing what is widely recognised as being the minimum level of vote privacy protection.

Verifying that the vote is cast as intended

The most difficult part of an Internet voting system to secure is the voter’s client machine. Ordinary PCs are notoriously insecure, and we would have to expect that many voters would cast their vote from a machine infected with malware or (legitimately or not) controlled by another person. If the machine used to cast the vote runs a program other than the intended program, it could submit a vote completely different from the one the voter requested. There would be no obvious way for the voter to detect this. A procedure for querying the computer would not prove anything, because a computer running malware could simply respond with a lie to the query, and tell the voter that it had submitted the correct vote when it had actually submitted something different. For example, a recent challenge to the Estonian voting system consisted of demonstrating a program that could present the appearance of a successful voting experience for a particular candidate, while actually casting a vote for a different one (Rikken, 2011). This was not a security vulnerability in the voting software itself, but a response to the inherent vulnerability of an ordinary PC.[2] The iVote system would be vulnerable to exactly the same kind of attack. The difficulty of ensuring that the vote is cast as the voter intended from a possibly insecure machine is the main reason that postal ballots

[2] The attack would apply also to Internet banking, but it would be easier to detect because the bank could contact the voter to discuss the contents of the transaction, as many banks do automatically by email or SMS. This is impossible for Internet voting due to privacy concerns.

are more secure than Internet votes for sighted voters. When casting a postal vote, the voter can see what vote is cast; when casting an Internet vote they cannot.

Many electronic voting vendors and promoters like to reassure voters that they have some guarantee that their vote was successfully sent, received and counted. This often takes the form of some sort of receipt or tracking number which voters can look up after voting. Unfortunately the appearance of a tracking number on a website proves very little about whether the vote was cast as the voter intended, received correctly and properly tallied. As we wrote in our submission to the 2007 inquiry, at best this query could detect some kinds of inadvertent errors, but this is not really a security feature. Most of the attacks that would cause votes to be misrecorded, altered or miscounted could just as easily attack the "verification" system too, resulting in a correct "verification" even when there had been an error.

For example, the iVote approved procedures Section 4.8.2 reads:

> *"1 The iVote system provides the voter a receipt at the conclusion of their voting session.*
> *...*
> *3 When the voter's iVote is decrypted, it will reproduce the same receipt number that confirms there has been no tampering to the vote. Should the vote be different to that which the voter has cast, the receipt number will be different."*

This makes no guarantee about whether the voter's intention was correctly expressed. Furthermore**,** tampering can occur at the voting client (before sending to the server), at the server (before the receipt number was generated), or after the receipt "verification". In all these cases the voter would still receive a correct receipt number from the "verification" process even when tampering occurred.

A similar criticism applies to the VEC's electronic receipt system for computers in polling stations in the 2010 Victorian state election, and to the receipt system for the overseas military personnel which was trialled in the 2007 federal election. For a more detailed explanation of exactly what the VEC's receipt system does or does not prove, see CORE's report: (Teague, (CORE, 2010)).

In summary, verifying that a vote cast from an insecure machine genuinely matches the voter's intention remains an unsolved problem for preferential voting by Internet. Dr Teague's current research focus is on designing systems that give some guarantees of integrity for preferential voting even on an untrusted client, but this is preliminary and at present the best systems are difficult to use and have other notable downsides. At present there is no secure and usable solution.

Computers in the Polling Station

Providing adequate security, privacy and transparency for freestanding computers in polling stations is quite feasible**.** In contrast to Internet voting, the controlled environment facilitates two vital security features:

1) the enforced privacy of a ballot box, and

2) the opportunity to provide a paper trail.

The integrity of the system can be demonstrated by designing the computers to print out a human-readable paper trail. A very good option is an "electronic ballot marking" system, in which the computer prints a real ballot which the voter then checks and places in an ordinary ballot box along with others' handwritten ballots. Another reasonable option, common in the United States, is a "Voter verifiable paper audit trail," (VVPAT) in which the primary record is the electronic one, but the paper printout is kept as a backup and checked against the electronic record. Generally not all of the VVPAT is recounted – some random selection is checked, with more checking the closer the election result. The point of both these systems is that the election's integrity is demonstrated by the paper record, not by placing trust in the correct functioning of the computer.

There are still challenges with these systems. The most obvious is that many electors who have difficulty writing on a piece of paper may also have trouble checking their printout or putting it in the ballot box. It is not known how to achieve meaningful integrity checking of computerised votes for blind voters (though some research exists). Perhaps it is best to acknowledge a tradeoff between accessibility and security, and design a system that could print either a human-readable paper trail (for sighted voters) or a non-human-readable record (like EVACS does) for blind voters. This was discussed in our submission to the 2007 inquiry. Also, there is some evidence that ordinary voters are not very good at checking the correctness of their printouts, though to our knowledge there is no research on our Australian style of voting.

Preserving vote privacy is an important but solvable challenge. If an electronic record of the votes is maintained, then it must be carefully structured to avoid revealing information about the votes.

Nevertheless a paper trail that voters have had at least the opportunity to verify would be a privacy-preserving method of achieving a high degree of integrity and transparency.

Recommendation 5: Secure voting by computer in the polling place is feasible provided it has a human-readable paper trail for sighted voters.

Other comments

Setting the scope

One serious problem that occurred both in NSW and Victoria's electronic voting solutions was that a system originally designed and justified on the grounds of giving an independent vote to visually impaired people was later expanded to a much larger population of voters without being redesigned appropriately. In the case of Victoria, a polling-place electronic voting system was designed without a paper trail because it was intended only for the blind, and then when it was expanded the paper trail was not implemented. This resulted in a system not nearly as verifiable as it easily could have been. The problem was that the original specification did not match its eventual use.

Similarly, the iVote system in NSW was originally promoted as being for a restricted set of voters and only much later expanded to include a much larger number of overseas and interstate voters, many of whom would have been perfectly capable of completing an early vote or a postal vote. The tradeoffs of security for convenience for this group are completely different from the tradeoffs for the visually impaired, and the implications of security vulnerabilities in the taking of nearly 50000 votes are considerably more serious than in the case of only the few thousand originally expected.

Verifying the Tally

Assuming (and it is a big assumption) that the input list of encrypted votes is valid, there is still the important point of proving that the votes have been decrypted and printed or counted correctly.

This applies to (remote) Internet voting and also to polling place electronic voting without a paper trail. Again there are some sound cryptographic techniques for proving the correctness of the decryption and counting step. However, preferential tallying solutions remain computationally expensive. Also the link between the cryptographic system and the main (paper) vote count needs to be considered. Some systems simply print out paper ballots, in which case it suffices to prove that the votes have been correctly decrypted.

Some comments about the AEC/Blind citizens Australia proposal, as described in Submission 56 (Zammit, 2011)

We do not understand the purpose of stage 2, in which a person is replaced by a computer. We see no reason to believe that this is a more private or more reliable scheme than stage 1.

Also, the telephone infrastructure is no longer in practice separate from, or more secure than, the Internet infrastructure. Voters may choose to "telephone" via skype, or via a sophisticated mobile telephone that is really a computer. Hence many of the security issues associated with remote computerised voting would apply to remote telephone voting too. Indeed, some kinds of security such as encryption of the communication channel are actually easier to control via a computer interface than from a telephone.

Summary of recommendations

1. Computerised voting systems, including their source code, all documentation and reports, and the associated physical security procedures should be available to e-voting and security experts and the public.

2. It should be recognised that the systems designed to address the unique usability and integrity concerns of visually impaired voters are not necessarily appropriate solutions for others.

3. We should consider alternative methods of using the communications infrastructure without necessarily trusting it alone to carry completed ballots.

4. If Internet voting is introduced, it should be only with the clear public explanation that the privacy and integrity of the system are significantly below those of postal voting. It is a last resort with limited integrity guarantees, appropriate at best for those who do not get high integrity or privacy guarantees with alternative systems. This does not include ordinary postal voters.

5. Secure voting by computer in the polling place is feasible provided it has a human-readable paper trail for sighted voters.

References

Teague, Vanessa. CORE, V. T. (2010). *Report on the VEC-Scytl electronic voting system for the 2010 Victorian Election.* Retrieved from Soon to be available online

Kennedy, A. (2011). *Submission 37.* Retrieved from JSCEM Inquiry 2010 Submissions: http://www.aph.gov.au/house/committee/em/elect10/subs/Sub037.pdf

Rikken, K. (2011, 3 10). *Student Finds Flaw in E-Voting, Seeks Nullification of Result.* Retrieved from ERR News - Estonian public broadcasting: http://news.err.ee/sci-tech/ed695579-af05-48ab-8cc0-3085e5f0c56c

Rivest, R. (2010). *Thoughts on UOCAVA Voting.* Retrieved 2010, from NIST workshop on UOCAVA voting systems: http://csrc.nist.gov/groups/ST/UOCAVA/2010/Presentations/RIVEST_2010-08-05-uocava.pdf

Wagner, D. (2010). *Overview of and Perspectives on UOCAVA Voting.* Retrieved 2010, from NIST Workshop on UOCAVA voting systems: http://csrc.nist.gov/groups/ST/UOCAVA/2010/Presentations/WAGNER_UOCAVA2010.pdf

Zammit, J. o. (2011, 2). *Submission 56.* Retrieved from JSCEM inquiry 2010 submissions: http://www.aph.gov.au/house/committee/em/elect10/subs/Sub056.pdf