Supplementary 116.1

COmputing
Research
& Education

Supplement to the 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. The public part of 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.

After CORE's first submission to the inquiry, which called for the publication of the e-voting systems' audit reports, the AEC mailed the audit reports to Dr Teague. This is a supplementary submission containing a detailed response to those audit reports. The last section of this submission, "Some specific issues about the audit report on eLect", should remain confidential because it provides details of the audit report, which the AEC wishes to remain confidential. That section should be publicised only if the AEC clears it.

Main findings and recommendations

1. The auditors' reports should be public, and the source code should be available to a much wider group of experts for analysis.
2. Whenever possible, the voter should have direct verification that their vote was cast as they intended and included correctly in the count (this is particularly difficult for visually-impaired voters).
3. There is inadequate evidence that the eLect system is secure.

Why the audit reports should be public and the source code more widely available

It is a common fallacy that secrecy makes electronic systems more secure.

The audit report on the eLect system does indeed suggest a host of security vulnerabilities, *but these are inherent in the system and would have been there even if the report were secret*. Keeping the audit report and the source code secret does not protect the system's security problems from exploitation, it merely prevents experts from identifying and ameliorating them.

It does not make sense for public trust in these systems to rest on the auditors' reports, when the public are not allowed to see those reports. Even if both reports were perfectly convincing, why would the public or the candidates be convinced by an analysis they were not allowed to read, of a system that not even their nominated representatives were allowed to scrutinise?

Public confidence in the systems would be greatly improved if more security experts were able to read the source code. Such experts could be engaged by the AEC and based in universities or relevant industries, or they could be nominated by candidates just as existing scrutineers are. Again there is a strong analogy with scrutineers of the paper counting process. Most voters never bother to act as scrutineers; their trust in that process is based on the knowledge that their preferred candidate(s) have nominated scrutineers to act for them.

Why voter-verification is necessary

Even if the source code were widely scrutinised it would be impossible for voters to verify that the program running on the computer were the same as the certified one. This is true whether the computer is administered by the electoral authorities and held in a ballot box, or owned by the voter and connected to a network. In the former case almost any step in the chain could change the program running on the computer: the vendors could provide executable code that did not perfectly match the certified version (perhaps for a perfectly sound reason such as a security update or bug fix), the installers could insert the wrong CD into the machine, the machine vendors could configure it incorrectly, or a hacker could attack the machine after installation. The point is that the voter has many people to trust and no direct evidence that they have all done their jobs perfectly. If the voter uses their own machine over a network, the problem is even more serious. They may be vulnerable to viruses, worms and phishing attacks that would cause them accidentally to run the wrong program. In both cases a clever hacker could arrange for the substitution to be totally undetectable, because he or she could also circumvent the electronic verification processes that are part of the same software—a hacker could install a program that lied to the voter about what vote had been

cast. The whole issue can only be addressed by direct voter-verifiability, allowing the voter to check that the correct vote was recorded on their behalf.

Voter-verification for computers in ballot boxes (eVacs)

The audit report on the system for visually impaired voters does not adequately address the issue of whether the recorded barcode always matches the voter's intention, except to say that they tested it and did not notice any errors. If such a system were to be extended to sighted voters, it should be required to provide voter-verifiability, meaning that the voter could check directly that the correct vote was being recorded on paper[1].

Obviously direct verification by visually-impaired voters is very difficult. The next-best form of assurance is regular testing *throughout the voting process* by officials and scrutineers, as described in my original submission.

Voter-verification over a network (eLect)

The eLect system provides a voter with no evidence that their vote was recorded correctly. The fact that the system provides a vote checking service, convinces the voter that *something* was recorded on their behalf, but provides no evidence of whether the vote that was recorded matched the voter's intentions. It is very unclear how the system could provide such verification without violating the voters' privacy. (There are some sophisticated cryptographic schemes for Internet voting that do provide verification while also resisting coercion, but to the best of my knowledge none of them allow preferential voting.) Postal voting, despite its imperfections, at least allows the voter to see what vote goes into the envelope. Hence it is much more secure than eLect.

Why the audit report on eLect is unconvincing

First some comments on security analysis. In order to be convinced that a system is secure, the argument must include the entire system, because an error at any point could result in the entire system being compromised. For example, if a particular item of data is encrypted at some point, then that may not be sufficient to keep it secret. The decryption key may be exposed, or the encryption algorithm may be weak, or the data item itself may be recorded elsewhere. We need to understand the whole system in order to understand whether it is secure. The audit report provides almost no details about how the eLect system works, and consequently no assurance that it works correctly and is secure. It contains sprinkled hints about security features, but no description of the system's structure.

The most disturbing aspect of this report is that it makes no mention of having inspected the source code for security vulnerabilities. Instead the source code evaluation focused on detecting deliberately malicious code within the source itself. Although this is important, it is far more likely that the designers and programmers accidentally left security holes that could be exploited by an external hacker. Such vulnerabilities would not be obvious from even quite extensive testing (though such testing is also important), because they would be extremely subtle. It is vitally important for experts to inspect the source code and evaluate the design, and thus form an argument about why the system is secure. Designing and evaluating secure software is notoriously

---

[1] Some sophisticated cryptographic schemes provide voter-verifiability without printing out a human-readable ballot. The important issue remains the same: that voters should be convinced of the correctness of their vote without having to trust the computer.

difficult. Even under considerable expert scrutiny, some vulnerabilities may still slip past unnoticed. (In 2007, CERT catalogued 7,236 security vulnerabilities in deployed software.) That the audit report does not even mention attempting this kind of analysis is very unfortunate. Their comment that the system was "designed, written and documented in a manner that could broadly be described as industry standard" is not encouraging.

The auditors attempt to deal with this issue in section 10.1 (Security Risks), item S3, "The applications running on the server are interfered with and now contain malicious code." The defence against this problem is "Inspection of relevant source code found no evidence of malicious software. The versions of software running on the server have been verified by the auditor. The system hardware is currently "locked down" in a secure area to prevent unauthorized access." All of this is an argument about why the auditors believe that the system, when initially deployed, does not contain malicious code. It does not even address the question of whether the system is difficult for a hacker to "interfere with" in order to run malicious code.

The rest of this submission details my particular concerns about the contents of the audit report on eLect. Since I was not authorised by the AEC to publicise any details about that report, the following pages should be secret. (Note that I have no wish to keep my comments secret, so if the AEC clears those pages for publication then I would happy for them to be published.)

Contact details

Dr Vanessa Teague

Declaration

My husband was an independent candidate for the Senate in the 2007 Federal election. It was as his scrutineer that I was able to observe the electronic voting process for visually impaired voters.

Some specific issues about the audit report on eLect (confidential)

The audit report contains occasional hints about the system's security features, which often generate more questions than they answer. They often refer to "testing" to prove something that should be demonstrated by a security analysis of the source code. Here is a sample of the comments that are particularly unclear.

Changing the configuration setup

Section 9 (process and procedures), item (e) reads: "The AEC will prevent personnel from making any changes to the configuration setup of an election while the election is open for voting." One certainly hopes that they will, because changing the "configuration setup" could affect the outcome of the election. It then explains that they will achieve this by disconnecting the Election Officer's PC (EOPC) from the Defence Server, but there is not the slightest hint of why this achieves the desired aim. Indeed, it is extremely unusual for such authentication to be vested in the identity of a PC. Much more common would be to ensure that only the possessor of a particular password or secret key was able to be authenticated (and for an application as important as this it would be common to share that secret key among several trustworthy individuals so that a quorum was required to actually make changes). How does the Defence Server authenticate the EOPC? How does it authenticate the person using the EOPC? How are malicious parties prevented from deceiving the Defence Server and pretending that their computer is the EOPC?

Item (f) adds to the mystery. It recommends that the AEC "save all logs to the EOPC when they are created to prevent them from being overwritten." Presumably these logs are generated by the Defence Server, which has been carefully disconnected from the EOPC according to the instructions in item (e). How will the logs get to the EOPC? Why will this stop them from being overwritten? (Wouldn't it be more effective to write them onto some non-erasable medium such as a write-once CD?)

Substituting the recorded votes

Security Risks S6 (from section 10.1) considers whether "The recorded votes on the eLect database could be substituted by a modified set of votes." Obviously this is a crucial issue, because vote substitution could change the vote tally completely. The treatment for this is firstly that "Votes are encrypted with a public key and are stored encrypted on the database and cannot be decrypted without a quorum of AEC officials being present." This may be good for vote *secrecy*, but it is completely irrelevant to whether votes can be substituted illicitly, because they could be substituted without being decrypted. The second sentence does not help. It states that the encryption is "tamper evident and cannot be altered." "Tamper evident encryption" is not a well-recognised term; tamper evidence is usually a property of hardware devices, so its use here is confusing. The usual technique to use in this case is message authentication, either an H-MAC or a digital signature. Again the reader is left unconvinced that a properly-chosen secure algorithm was used.

Identifying which individual cast a particular vote

It is important for an electronic system to dissociate particular voters from their votes, as our paper-based system does via a ballot box in which a number of paper ballots are mixed. The audit report considers this problem (Security Risk S8, section 10.1), and provides two arguments. The first paragraph claims that "The vote data does not associate the voter with the votes." This is perfectly

reasonable, since it would be possible to design an electronic voting system that simply never recorded the voter's identity and their vote together. (The Victorian Electoral Commission's system for visually impaired voters, for example, was designed so that the voter never communicated their identity to the computer.) But the second paragraph directly contradicts this: "When the ballots are decoded by AEC personnel, they are then handled according to existing AEC procedures for postal ballots to protect the secrecy of the votes through separation of the votes from the voter information." Why do they need to be separated if they are never associated in the first place? The last sentence reiterates the first claim: "These two sets of data are downloaded and processed separately." This makes no sense.