The Secretary
Joint Standing Committee on Electoral Matters
Parliament House
CANBERRA, ACT 2600

Inquiry into the 2001 Federal Election

Submission by: John Rogers[1] BSc, MACS, LIMA

Summary

1. This submission relates to the use of computer programs and similar electronic means to record and count votes, and distribute preferences in Federal Elections.

The Present Situation

2. It is submitted that the computer program employed during the 2001 Federal Election for the distribution of Senate preferences:

    - was ***not*** written to appropriate *Trusted Computing*[2]standards;
    - was ***not*** independently validated for correctness of operation by a body recognised as competent in the field; and
    - was opaque in its operation to the candidates and the electorate at large.

    As a result, although there is no evidence that votes were incorrectly distributed, the possibility exists that this was the case due to:

    - some accidental and undetected fault in the program; or
    - the malicious action of a programmer.

Proposed Action

3. It is suggested that the Joint Committee recommend to Parliament that all future computer programs and similar electronic means of counting, recording, and distributing votes in Federal Elections be written and evaluated to meet the international standards for mission-critical and secure Trusted Computing.

4. It is further suggested that full details of any Voting System be made public so that voters are once again able to verify personally that the process is in accordance with law. However the desirability of doing so must be balanced against the risk that a malicious person might discover and exploit an unnoticed loophole. As an alternative a committee of well-known and independent experts could be asked to certify the appropriateness of the System and its employment.

[1] Short biography as evidence of expertise appears as Attachment 1 with my contact details.

[2] *Trusted Computing* is a technical information technology term relating to the quality of computer programs – see para 13-17 below.

Background

The Problem

5. When votes are on paper the voter is sure of how his/her vote has been recorded. Further, when paper votes are counted and distributed it is clear to the candidates and any other observers that the process has been performed correctly. Recounts are possible and, in extreme cases, examination of the ballot papers can establish that all the forms were validly issued.

6. Electronic voting programs make all these processes opaque. The voter cannot see whether her/his vote is correctly recorded or even recorded at all. Candidates and others cannot see the votes counted: they must simply trust the computer's processing. Recounts are simply a repeat of the original counting process and cannot detect errors. There are no ballot papers to verify that all the votes were made by electors: unless special measures are taken there is nothing to establish that the electronic records are a true statement of the voters' intentions.

7. It is a matter of everyday experience that computer programs often fail to function exactly as expected or desired. Electronic voting was employed during the 2001 ACT Assembly Election and, according to the *Canberra Times* of 29 October 2001, a 'bug' delayed publication of the results so it is apparent that that voting program in particular contained errors. Given that 'the slightest difference in the votes would have changed the results' (Canberra Times, 2 November 2001), there can be no certainty in this case that the candidates who were declared successful were in fact duly elected.

8. The reason computer programs often contain 'bugs' is their complexity. This makes it difficult for the programmer to ensure the correctness of what is written and even harder for another person to check the logic. This can be further aggravated by difficulties in understanding what the program is expected to do. Thus if the programmer fails to understand exactly how, for example, preferences are to be distributed, the program is likely to contain errors. The complexity and difficulty of checking computer programs also provides the opportunity for a malicious programmer to include mechanisms to bias the result.

9. Most computer programs, and certainly that which distributed the 2001 Senate Preferences, are extensively tested before actual use. However testing is not sufficient to determine a program's correct operation under all conditions. In the information technology industry it is well-known that testing simply shows that *anticipated* errors have been avoided. It does not demonstrate the absence of unexpected errors. Exhaustive testing, which *might* achieve the desired result, is never possible because the number of trials involved is too great.

10. *Hacking*, ie. illicitly entering computer systems via their communications networks, is a frequent occurrence as the Australian Federal Police (AFP), the

Australian Security Intelligence Organisation (ASIO), and Defence Signals Directorate (DSD) can attest. Existing operating and network systems (eg. Microsoft Windows) typically offer only limited protection against hacking attacks. Thus, if the Senate preference distribution program was run on a networked computer, even if the network was wholly contained within the Australian Electoral Commission (AEC), it was open to a malicious person to attempt to hack into and modify the program or the stored votes so as to change the outcome of the Election.

11. Hacking could, unless appropriate precautions are taken, become a major threat if electronic voting machines were introduced at some future date to record and count votes at the polling booth, especially if the results are returned to the AEC via electronic communications systems.

12. In summary:

    a. Electronic voting systems make the voting process opaque to the candidates and the general public.

    b. They may not give the correct outcome of an election because:

        - the computer programs may contain accidental errors;
        - illicit instructions could be included in the programs by a malicious programmer; and
        - a malicious person could gain access (possibly by hacking) and modify a program at any time between it being written and it being used.

    c. In-house testing is insufficient to overcome these problems.

The Proposed Solution

A. *Programming Deficiencies*

13. Methods have been developed to build computer systems in a way which minimises the likelihood of them containing any errors, accidental or deliberate, and of securing them against modification up to and during their deployment. The driving force has been the need for correct and inviolable systems for reasons of safety (eg. air traffic control), security (protection of classified information), and mission criticality. The use of these methods is termed *Trusted Computing.*

14. Trusted Computing is rarely used in commercial and other 'ordinary' computing applications because it is little known (few universities teach it in any detail), is initially more costly than conventional methods, and may be considered disproportionate to the risks ordinary business enterprises face. Broadly the methods of Trusted Computing require:

- a detailed description, often expressed in terms of formal logic, of the problem;
- the application of special procedures to the design, construction, and testing of the computing system;
- provisions for protecting the integrity of the system once written, including mechanisms to detect changes to it;
- independent validation of the whole process including a detailed examination of the programs by an independent team of expert evaluators.

15. The infrastructure for Trusted Computing is well developed, both internationally and in Australia. There is an international standard, *ISO15408: the Common Criteria for Information Technology Security Evaluation,* and the Commonwealth Government has a programme, *the Australasian Information Security Evaluation Programme*, in place to assess computer products and systems against the standards (for further details see http://www.dsd.gov.au/infosec). For certain security purposes it is mandatory for Commonwealth Government Departments to use products evaluated under this scheme. In the arena of safety and mission criticality the University of Queensland's Software Verification Research Centre has well-developed facilities (see http://www.svrc.uq.edu.au - particularly the list of projects past and present), and the National Association of Testing Authorities (http://www.nata.asn.au) is working in the area.

16. To meet the deficiencies identified above in the Senate preference distribution program and to avoid problems with future voting systems, all Federal Government voting systems should be treated as both mission critical (ie. they must be build to work correctly) and security critical (ie. they should be resistant to malicious attack). The facilities exist to achieve this and they should be used.

17. The Defence Signals Directorate and the University of Queensland's Software Verification Research Centre would be in a position to advise the Joint Committee on how the proposed scheme could be implemented, and to assist the AEC in doing so.

B. Opacity

18. To make electronic voting wholly transparent it would be optimal to place on the public record complete listing of all the programs and the operational documents. However this must be balanced against the potential for a malicious person to search for and exploit any undetected weakness in the system.

19. A second, less desirable but more secure, option would be to invite an independent group of acknowledged experts in the field to certify the process of building and operating Federal Government voting systems as appropriate for the purpose. Once the personnel of the Australian facilities are excluded to retain the independence aspect, the field from which this group could be drawn would be rather narrow, so inclusion of one or more international experts might be valuable.

4 July 2002

Attachment 1

John Rogers: Professional Biography

- 38 years in the Information Technology industry in both public service and private industry.

- 1962-77: Government Communications Headquarters (UK)
    - heavy involvement in communications security

- 1986-99: Defence Signals Directorate (DSD) (Australia)
    - founder of the Commonwealth Government's Computer Security Authority
    - original author of *ACSI-33*, the Commonwealth's technical computer security guide
    - major contributor to the Commonwealth's *Protective Security Manual*
    - initiator of the *Australasian Information Security Evaluation Programme*
    - founder member of the interdepartmental committee for the Protection of the Information Infrastructure
    - heavily involved in the development of *Gatekeeper*, the Government's Public Key Infrastructure (PKI) initiative
    - member of Standards Australia's information security and PKI committees.

- B.Sc in Mathematics
- Member of the Australian Computer Society
- Licentiate of the Institute of Mathematics and its Applications

- Australian Intelligence Community medallion for distinguished service, 1999.

Since August, 1999, I have been retired from full-time work although I undertake the occasional consultancy in information security and contribute to various workshops and seminars.

I have no financial or similar connection with any business or organisation who might benefit should my proposal to the Joint Committee be implemented.

4 July 2002

Contact Details

John Rogers