Review— Second Report of the Irish Commission on Electronic Voting

Jonathan Lundell
jlundell@pobox.com

1 Introduction

> . . . the Commission concludes that it can recommend the voting and counting equipment for use at elections in Ireland, subject to further work it has also recommended, but that it is unable to recommend the election management software for such use.

So reads the conclusion of the Irish Commission on Electronic Voting [1].

The government of Ireland chose an electronic voting system for use beginning with the local and European Parliamentary elections of 11 June 2004. Responding to public criticism, the government established the Independent Commission on Electronic Voting and Counting at Elections in March 2004 [2]. In April 2004, the Commission issued an interim report recommending against using the chosen system for the 2004 elections, citing concerns over secrecy, accuracy and testing. The Commission issued its First Report in December 2004, and its Second (and final) Report in July 2006; the Commission was dissolved in September 2006. Except for a limited pilot test in 2002, the system has not been deployed.

In addition to recommending further work on the voting equipment, and replacement of the election management software, the Commission recommended changes to the overall operation of the elections system, including better physical security for the machinery itself, and noted that more testing will be required:

> The testing of the system as a whole carried out to date, as well as the investigation, analysis and independent testing and certification of its individual components, is insufficient to provide a secure basis for the use of the system at elections in Ireland. There is thus a need for comprehensive, independent and rigorous end-to-end testing, verification and certification by a single accredited body of the entire system as proposed for use in Ireland. While the Commission's work has laid the foundations for this process, more work will be required in this area ([1] p8).

The Second Report runs to more than 350 pages, not including much supplementary information available on the Commission's website: public submissions, technical information on the chosen system, and more. An adequate summary of the report is beyond the scope of this review, but the report itself is quite readable; the interested reader would do well to begin with the report's summary and conclusions ([1] Part 7).

This review generally confirms the judgment of the Commission, but, based on additional information, questions the Commission's conclusion that the chosen system can be made acceptable with further work.

2 The chosen system: hardware

The voter sees a series of up to five paper ballots behind transparent plastic. Each paper ballot lists up to 14 candidates, and beside each candidate is a button and a numeric LED display. In an STV election, the voter presses the candidate buttons in order of preference, and the numeric displays reflect the preference order. When all preferences have been entered, the voter presses another button to record the ballot in a removable nonvolatile memory (Ballot Module) installed in the Voting Machine.

A small LCD screen provides feedback and instructions to the voters. A cable connects the Vot-

For this publication, see www.votingmatters.org.uk

ing Machine to a separate control unit, used by the polling station staff to control the Voting Machine and monitor its operation.

After the close of voting, the Ballot Module is physically transferred from the Voting Machine to a Programming and Reading Unit (PRU) connected to a PC that runs software to read the ballot data and transfer it to a CD for consolidation with ballot data from other machines to be counted.

(The PRU is also used before the election to write information to the Ballot Module that the Voting Machine uses to configure itself, including a description of the layout of the paper ballots affixed to the Voting Machine, with the names of the candidates, which are also displayed to the voter on the LCD screen as voting buttons are pressed.)

The CDs containing ballot information are transported to a central facility where they are read, aggregated, and counted ([1] Part 3.2).

3 The chosen system: software

The Voting Machine software, written in ANSI C, runs on the PRU as well as the Voting Machine.

The "Integrated Election Software" (IES) runs on a "hardened" PC running Microsoft Windows 2000. Written in Delphi, Borland's Object Pascal, IES consists of modules for STV counting, election management, and management of the PRU. In addition, IES uses several third-party tools and libraries, including the Microsoft Access database system.

The Voting Machine software comprises some 25,000 lines of code, while IES approaches 100,000 lines, of which some 40,000 lines are devoted to the counting module ([1] Part 3.2).

4 Public comments

The Commission invited submissions from the public, and has published them on its website. Submissions were received from a variety of sources, including private individuals, opposition parties, voting-system advocacy groups, and the Irish Computer Society. Common to most of the submissions is an insistence on a voter-verifiable audit trail (VVAT).

5 Vendor comments

The Second Report includes an extensive response from Nedap NV, the Dutch vendor of the chosen system. Nedap generally takes the position that the chosen system as supplied conforms to their contract, and that it is trustworthy and secure. Nedap argues that a voter-verifiable paper audit trail (VVPAT) is not just unnecessary but actually undesirable, and argues that an open-source voting system (ie, one in which the details of the hardware and software implementations are made public) is undesirable as well.

Nedap cites a paper by Selker and Goler [3] criticizing VVPAT. However, the paper in question actually advocates VVAT but considers VVPAT inferior to alternative approaches to VVAT (Selker advocates a voter-verified audio audit transcript trail (VVAATT) in which the voter verifies an audio transcript of his or her choices; the audio transcript is recorded for use in a possible audit [4]).

Nedap and their Irish branch, Powervote Ireland LTD, assert that the system has already been adequately tested:

> The hardware and software of the VM, PRU and BM were analysed and tested by the accredited German "Physikalisch Technische Bundesanstalt" who is the body that is appointed by German law to analyse and test electronic voting systems before they can be deployed in Germany ([1] p290).

With respect to the Integrated Election Software,

> The Integrated Election Software can be divided into 3 main sections:
>
> 1. Preparation and Administration
> 2. Programming and reading in ballot modules
> 3. The Count
>
> Sections 1 and 2 have been in use in other countries for many years. Millions of votes have been processed and counted without incident or challenge. These 2 crucial sections are therefore very well proven in practice and form part of the Irish version.
>
> Unlike Sections 1 and 2, Section 3 was developed specifically for Ireland. This was subjected to extensive testing by the Department prior to its deployment at the Dáil election and the Nice referendum. IES is a mature and stable design. Adaptations and enhancements are inevitable for each new country. Changes to electoral practices are common and require software which can be

> readily adapted to meet these changing requirements in a very timely way. Each time a change is introduced requires testing to be carried out.
>
> Once testing is completed satisfactorily then that particular build number is not allowed to be changed and is issued for use ([1] p362).

6 "We don't trust voting computers"

Since the Commission's Second Report was issued, the Dutch group "Wij vertrouwen stemcomputers niet" ("We don't trust voting computers") has demonstrated the ability to compromise the Nedap voting equipment used in the Netherlands [5]. In response, the Dutch government has mandated security changes to their voting machines in advance of their November elections [6]. The Dutch voting equipment is essentially similar to Ireland's chosen system, and it's likely that the chosen system has similar vulnerabilities.

7 Comparative assessment against paper voting

The Irish government added to the Commission's tasks a "comparative assessment of the security and accuracy of the current system (ie, the paper-based system) for voting at elections and referenda." ([1] p147). The Commission found that the paper system is "moderately superior overall" to the chosen system as it currently exists, but that if all the concerns of the Commission could be addressed, the chosen system as improved would be superior to the paper system.

Not addressed is the question of whether the potential benefits of the chosen system outweigh its cost of acquisition and ongoing overhead, as well as the less tangible cost of the potential loss of confidence of Ireland's voters in its elections, a consequence suggested by the public comments.

8 VVAT

A voter-verifiable audit trail (VVAT) is intended to provide a means, independent of the integrity of the voting machinery in use, 1) to determine whether the election was accurately recorded and reported and 2) to provide an independent means of recounting the election should the accuracy of the electronic voting machinery be called into question.

A VVAT is typically accomplished by printing a paper record of each voter's ballot in such a way that the voter can verify that the paper record is correct, while not permitting the voter to retain a copy (which would be contrary to the secrecy requirement). The paper record is then used to spot-check the electronic results and, if necessary, to serve as the basis of a recount.

Implementation of an effective VVPAT is nontrivial, requiring among other things that an adequate proportion of voters actually check the paper record in detail, so that discrepancies are detected, and that a statistically adequate sample of paper ballots be counted to have good assurance that the electronic count is correct. Selker [4] advocates a "voter-verifiable audio audit transcript trail" (VVAATT) instead of a paper trail, but this approach has drawbacks of its own, being more difficult to audit.

9 NIST Discussion Draft

In 2002, US federal legislation [7] effectively mandated electronic voting equipment as a means of correcting election-systems deficiencies that came to light in the 2000 US presidential election, as well as of allowing more disabled voters to vote without assistance. The law charged the National Institute of Standards and Technology (NIST) with assisting in the development of technical guidelines for voting systems. In November 2006, NIST issued a draft document concerned with the upcoming 2007 update of the US federal guidelines. The NIST draft is unequivocal in its opinion of electronic voting systems without independent audit trails.

One conclusion drawn by NIST is that the lack of an independent audit capability in DRE [direct record electronic] voting systems is one of the main reasons behind continued questions about voting system security and diminished public confidence in elections. NIST does not know how to write testable requirements to make DREs secure, and NIST's recommendation ... is that the DRE in practical terms cannot be made secure [8].

One of the central themes in the debate over voting system approaches such as the DRE is whether the level of certainty in the DRE is still adequate to ensure that the records have been recorded correctly. ... Trust in an election outcome relies heavily upon trusting the correctness of the DRE's software and upon trusting that the DRE software has not been replaced nor tampered with. But, assuring software correctness and security is very difficult and expensive, and techniques for doing this are still an open

research topic. ...Simply put, the DRE architecture's inability to provide for independent audits of its electronic records makes it a poor choice for an environment in which detecting errors and fraud is important ([8] p7).

Are there ways to improve DREs so that they can be made secure and fully auditable? NIST and the STS do not know how to write testable requirements to satisfy that the software in a DRE is correct. The use of COTS [commercial off-the-shelf] software in DREs causes additional problems; having, for example, a large opaque COTS operating system to evaluate in addition to the voting system software is not feasible ([8] p9).

(In the context of the chosen system, "COTS" includes Microsoft Windows, the Microsoft Access database system, and the Borland Delphi software development environment.)

According to the NIST, 35 of 50 US states use voter-verifiable paper records entirely, and another 10 states use them on a county-by-county basis. Only five states now use DRE with no paper trail statewide.

10 Commentary

My own background is in the design and manufacture of computer systems, and I find the Commission's conclusions on hardware and software quality all too plausible, though the proprietary nature of the chosen system's software makes it impossible for me to independently verify the Commission's conclusions.

The Commission suggests that the defects of the chosen system could be remedied, in part by completely rewriting the IES election management and counting software. It seems likely that the Commission, had its remit included a determination of best practices, would have seriously considered a requirement for a VVAT of some kind.

The Irish government's selection of an electronic voting system of any kind was in retrospect premature. Such systems have received much attention recently, especially in the US, and the technology is in flux. In any case, the Commission's comparison of the chosen system with paper ballots does not make a compelling case for a change to electronic voting.

One of the difficulties in completely auditing the chosen system lies in being able to guarantee that the software running in binary form on each voting machine, as well as the IES systems, corresponds exactly to the software examined in source form by the auditors. It must be possible for a signed and certified copy of the original source code to be compiled independently into a signed and certified binary copy of the code, and in turn to be able to guarantee that the software running on the voting systems is in fact a faithful copy of the certified binary. This is complicated by the fact that the IES is critically dependent on third-party software such as Microsoft Windows and the Microsoft Access database system, as well as the Borland Delphi software development environment, none of which has been independently audited.

While some of these difficulties can be mitigated, and others entirely corrected, it is impractical, if not impossible, to be able to guarantee that any electronic voting system is completely trustworthy and, as important, is seen to be trustworthy. The fact that a company with the resources of Microsoft has not been able to guarantee the security of its own web browser (let alone the entire Windows operating system) despite years of effort and large incentives, suggests that a fully secure and trustworthy electronic voting system may be an unattainable goal, especially given the complexity of the overall system and the incentives for subverting it, making an effective independent VVAT mandatory.

11 Options

The Irish government is left with several options for moving forward.

Adopt the Commission's recommendations. Improve the voting machine and its software, improve procedures during and between elections, and replace the IES with alternative software that can meet the Commission's standards.

Adopt the Commission's recommendations as above, but require the vendor to provide a voter-verifiable audit trail (VVAT), and adopt appropriate procedures for taking advantage of the VVAT.

Abandon the chosen system, begin a process to define new criteria for a voting system, and then identify and acquire such a system.

Abandon the chosen system and continue to use the existing paper-based system, perhaps with procedural improvements, leaving open the option of considering an electronic voting system at some future time.

The Sunday Business Post (Dublin) reports that the government is leaning toward option 1, estimating the cost of complying with the Commission's recommendations to be approximately €500K, compared with a sunk cost of some €60M. The €500K figure is disputed, however, and regard-

less of the cost of option 1, the cost of option 2 would be substantially higher [9].

My advice? Choose option 4, and establish a new commission that would, with public participation, recommend improvements to the present paper-ballot system, monitor the experience and (dis)satisfaction of other users of electronic voting systems, and develop criteria for the eventual selection of a system for Ireland. The world of electronic voting is evolving rapidly, and Ireland is in a fine position to take advantage of the experience (including the bad experience) of others before taking such an important step.

12 References

[1] *Second Report of the Commission on Electronic Voting on the Secrecy, Accuracy and Testing of the Chosen Electronic Voting System*. Independent Commission on Electronic Voting, July 2006, p7. http://www.cev.ie/htm/report/download_second.htm

[2] Terms of Reference and the several Reports of the Commission are available at http://www.cev.ie.

[3] Ted Selker & Jon Goler, *Security Vulnerabilities and Problems with VVPT*, CalTech/MIT Voting Technology Project White Paper #16, April 2004. Available via the McDougall web site.

[4] Ted Selker & Sharon Cohen, *An Active Approach to Voting Verification*, CalTech/MIT Voting Technology Project White Paper #28, May 2005. Available via the McDougall web site.

[5] Rop Gonggrijp et al, *Nedap/Groenendaal ES3B voting computer: a security analysis*, the "We do not trust voting computers" foundation, October 2006. Available via the McDougall web site.

[6] Aaron Gray-Block, "Fraud concerns over ballot computers", Expatica, 18 October 2006. Available via the McDougall web site.

[7] *Help America Vote Act of 2002*, United States Public Law 107-252. http://www.fec.gov/hava/law_ext.txt

[8] *Requiring Software Independence in VVSG 2007: STS Recommendations for the TGDC*, William Burr, John Kelsey, Rene Peralta, John Wack, National Institute of Standards and Technology, November 2006, p4. Available via the McDougall web site.

[9] Adam Maguire, "Fine Gael accuses Ahern on e-voting costs", Sunday Business Post Online, 29 October 2006.