Review— The Machinery of Democracy, Protecting Elections in an Electronic World

Brian Wichmann
Brian.Wichmann@bcs.org.uk

1 Introduction

The document being considered here [1] is a highly significant report which deserves careful study by those nervous about the security aspect of using computers for elections. The report is from a Task Force with many experts with established reputations in the field. Moreover, many others clearly performed studies for the Task Force, including the National Institute for Standards and Technology (NIST).

Equally important to the work were reviews and comments made by those professionally responsible for elections across the USA — Registrars and Auditors.

There are important limitations to the study, namely that the only voting systems considered were ones available at the time, and that postal voting was not considered. For the UK, this last restriction is important, since a recent legal case has indicated fundamental weaknesses in the UK postal voting system [2].

Lastly, this report is specifically written to address problems in the US system, and hence its application to other jurisdictions is for readers to decide.

2 The context

The US has thousands of electoral jurisdictions — many more than one per state. The number of jurisdictions that make their own decisions about voting procedures and equipment is smaller, but runs into hundreds. Hence the issues to be addressed are large and diverse due to the different technologies used. The report divides the electronic voting systems into three classes:

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

DRE Direct Recording Electronic. A DRE machine directly records the voter's selections in each contest, using a ballot that appears on a display screen. There are at least 9 types of machine like this.

DRE w/VVPT A DRE with Voter-Verified Paper Trail captures a voter's choice both internally in electronic form, and contemporaneously on paper. There are at least 5 machines of this type.

PCOS Precinct Count Optical Scan. PCOS voting machines allow voters to mark paper ballots, typically with pencils or pens, independent of any machine. Voters then carry their sleeved ballots to a scanner. At the scanner, they unsleeve the ballot and insert into the scanner, which optically records the vote. There are at least 3 systems of this type.

Note that all three types of voting systems need to be configured for a specific election. Undertaking this task implies access to the machine that could lead to security issues.

3 The methodology

Given the scale of the problem in the US, a methodology was needed to provide a framework for the work and ensure that the result could be understood without too much difficulty.

From existing electoral statistics from 10 states, an artificial state called Pennasota, was devised. The 10 states were all marginal making them potential targets for an electronic attack. The main analysis was for the Governor of Pennasota with the following voting pattern:

Candidate	Party	Total Votes	Percentage of Votes
Tom Jefferson	Dem-Rep	1,769,818	51.1
Johnny Adams	Federalists	1,689,650	48.8

In addition to the overall figures above, the split of the votes amongst the precincts and polling stations and voting machines was produced.

The next stage of the methodology was to produce a list of potential threats — 120 in all. These 120 were then analysed to identify the most important ones. The key to this part of the analysis was noting how many people would be needed to undertake a successful attack. The main conclusion from this was that threats against individual polling stations would be unlikely to be successful due to the number of stations needed to swing the Pennasota vote — 40,000 votes out of over 3 million.

There are two forms of analysis — one a generic one concerned with the nature of PC-based equipment, the other arising from the most important of the 120 identified threats.

Basing voting machines on PC technology has obvious problems due to the known security issues with both Windows and Linux. It seems that all the equipment considered use either of these two operating systems. Personally, I consider this inappropriate for polling station equipment since it would be difficult to ensure adequate security both at the polling stations and during storage and transport between elections.

Of course, validation and checking is undertaken of voting machine software. However, it seems this is limited to the software written for the purpose, rather than the entire system (which could be very large). This seems to imply that using the operating system to subvert the voting machine software is a credible line of attack. This supports my own contention that polling station machines should be like other embedded software systems — such as the systems used to control the engine of modern cars.

Another generic issue to be faced with all the equipment is the need to customise it for a specific election. For this purpose, ballot definition files are used. Hence an issue to be considered is whether changes to such a file could be undertaken with a view to changing the election result. Here the threat seems less credible.

3.1 Threat analysis

By way of illustration, we take the most credible attack on each of the three systems.

For the **DRE** system, this attack is a Trojan Horse inserted into the operating system. To remain undetected, it would probably have to be activated carefully so that testing prior to the election would not reveal the Trojan Horse, nor would the limited validation undertaken immediately prior to the election. To me, this attack seems very credible which is why I believe such machines should have embedded software and not rely upon a conventional operating system.

For the **DRE w/VVPT** system, a Trojan Horse again seems to be the most credible form of attack. The difference here is that there is a much more complex task since a paper trail needs to be produced as well. Since this paper record can be checked by the voter it probably means that success would depend upon the voter making no such check, which is usually the case. This threat seems much less credible than the previous one.

For the **PCOS** systems, a memory card is used to record the votes, and hence an attack on this is credible, as is the Trojan Horse attack yet again.

As another example of this analysis, consider the system to be used in Scotland for this year's local elections. Here, there are a small number of counting centres to which the ballot boxes are transported. Hence the security problem for **PCOS**-style machines at these centres is much easier to manage than having equipment at each polling station. Moreover, the process of transport and handling ballot boxes is well established. Hence, although an attack is not impossible it seems very much less credible than in the US context.

4 Conclusions

A large number of recommendations arise from the study: for instance, that no use should be made of wireless components due to the potential security threat. A feature of the analysis is the nature of counter-measures that would be effective against specific threats. Here, statistical analysis of results could reveal unusual voting patterns which could indicate an attack, or perhaps faults in equipment.

There is substantial evidence in this report that the validation, checking and counter-measures against a security threat were inadequate in practice. It seems unlikely that all of the detailed recommendations in the report could have been acted upon for the elections in November 2006.

For the position in Scotland using scanning equipment, the key issue would be how many informed participants it would take to perform a successful attack.

For those with any direct responsibility for elections involving electronic equipment, the report should be studied carefully — it is impossible to summarise the 147 pages adequately here — in any case, the key issues will depend upon the type of system being used.

(Further reports have been issued by the Brennan Center on Usability, Access and Cost of voting systems — these are not reviewed here.)

5 References

[1] THE MACHINERY OF DEMOCRACY: PROTECTING ELECTIONS IN AN ELECTRONIC WORLD. The Brennan Center Task Force on Voting System Security. www.brennancenter.org, 28th June 2006. (File date 8th August 2006)

[2] Dominic Kennedy and Jill Sherman. Postal voting is an invitation to fraud, says judge. *Times* 23rd March 2005. http://www.timesonline.co.uk/article/0,,2-1537754,00.html