NUI MAYNOOTH
Ollscoil na hÉireann Má Nuad

National University of Ireland, Maynooth
Maynooth, Co. Kildare, Ireland.

Department of Computer Science
Technical Report Series

NUIM-CS-TR2003-02

E-voting: a safety critical system

Margaret McGaley, J. Paul Gibson

Electronic Voting:
A Safety Critical System

Margaret McGaley, J. Paul Gibson
Department of Computer Science,
National University of Ireland, Maynooth

Date: March 2003

Technical Report: NUIM-CS-TR2003-02

Key words: Electronic voting, computer security, formal methods, safety critical

Abstract

This is a study of electronic voting, with emphasis on its implementation in the Republic of Ireland. We place electronic voting in its historical context, and define the basic requirements for any voting system. We examine remote electronic voting (REV) and kiosk voting – in particular the Nedap/Powervote system bought by the Irish government – to see if they can meet those requirements. We were motivated by a concern that the Nedap/Powervote system may not be a satisfactory solution to Irish electoral needs. Our conclusion is that while an adequate electronic voting system is possible, Nedap/Powervote is not it.

Introduction

"An observer of voting technology once remarked: 'If you think technology can solve our voting problems, then you don't understand the problems and you don't understand the technology.' "

– Dr. Rebecca Mercuri, Oct 2002 [1]

The Irish government has already begun to introduce an electronic voting system, stating that it will be easier to use, give more accurate results, eliminate spoiled votes, speed up the count, and modernise the electoral system [2]. Unfortunately, this system has been developed outside of the state, by a private company [3]. The wider computer science community has not been consulted in the choice or development of this system, and it has become apparent that there are several reasons to be concerned about the system chosen. There is no technical documentation regarding the system widely available, and what is available was clearly written with the computer-illiterate voter in mind [4]. The source code developed has not been made available, and contact with Mr. William Stapleton of the Franchise Section of the Department of the Environment and Local Government (DoELG) has confirmed that even they do not have a copy.

The aims of this report are to present a list of criteria that any electronic voting system must meet in order to make it an acceptable replacement for our current paper system, and then to demonstrate that the Nedap/Powervote system currently being introduced by the Irish government does not, in fact, meet those criteria.

To begin, it is necessary to put electronic voting in its historical context, both in terms of voting systems and technology. This will be followed with a development and presentation of the requisite criteria for any electronic system to ensure that it is at least as trustworthy as the paper system it replaces. Thirdly, an examination of Remote Electronic Voting in relation to the criteria developed will be made, and finally, we examine how a satisfactory kiosk voting system could be developed to meet the criteria previously discussed.

Historical and Philosophical Context

"'Many forms of Government have been tried, and will be tried in this world of sin and woe. No one pretends that democracy is perfect or all-wise. Indeed, it has been said that democracy is the worst form of Government except all those others that have been tried from time to time."

– Winston Churchill, Nov 1947

Democracy

We, in Ireland, live in a representative democracy. This means that the citizens of Ireland govern themselves by electing representatives to make decisions for them. From its origins in ancient Athens [5] to its current incarnation, democracy has gone through many changes. The number of people eligible to vote in a modern democracy is much greater than in ancient Athens, and so democracy cannot be used here in its original form. Not only are modern countries larger than the Greek city states, but many more categories of people are allowed to vote. As a result, gathering the electorate together for a discussion on the topic at hand is no longer possible. Nor, indeed, is allowing the whole electorate to vote on every issue. This is why we have moved from direct democracy to representative democracy.

However, the underlying principles that make democracy better than "all those others that have been tried from time to time" remain intact. The word itself comes from the Greek words 'demos' meaning 'people' and 'krátos' meaning 'authority' [6], and is commonly defined as meaning "government by the people". So, in a democracy the people make the decisions, if not directly then through the representatives they elect. This gives each voter a certain responsibility to adhere to the decisions reached through the democratic process [7]. It also gives citizens who are eligible to vote a responsibility to exercise their franchise, since they cannot complain about the result of decisions if they did not use their opportunity to affect them.

Manual Vote Collection

Of course, if an electorate is going to elect representatives, their decisions must be collected somehow. It would be impractical to use the Athenians' method – dropping clay balls (the origin of the word ballot [6]) into clay pots. And so we collect ballot papers, on which voters indicate their preferences. One of the major turning points in the development of modern democracy was the appearance in the 1850s of the Australian ballot. This is the name given to standardised ballots, issued by the government, with the names of all the running candidates already printed on them. As we use them today, Australian ballots allow us to separate the task of authenticating a voter from the task of authenticating a vote. This means that we can be sure that:

- only eligible voters vote,
- they only vote once, and
- all votes counted are valid votes.

All this can be achieved without allowing anyone to see who made any particular vote. Through the use of a polling station, we can protect against voter coercion and verifiable vote sale. But the most important aspect of our modern vote counting system is that at no point in the vote collection and tabulation process must we place our trust in an individual or small group of individuals. At every stage independent observers and representatives of interested parties are welcome to be present.

Electronic Vote Collection

This vote collection and tabulation process is, in fact, fundamental to our democracy. A country which was nominally democratic, but whose voting system was controlled by the "Powers That Be", might not be a safe place to live. Electronic voting systems (EVS) can therefore be classed as Safety Critical since a serious breach of their security could potentially put people's lives at risk.

In the past, it appears that governments worldwide and their respective electorates have been quite concerned with any changes implemented in their voting systems. Unfortunately, this is not the case with the switch from paper ballot voting to electronic voting systems [8]. In the rush to appear technologically advanced, inadequate voting systems are being installed and used. Significant errors and failures in voting systems since Florida 2002 have been noted by Dr. Rebecca Mercuri [9], one of the leading thinkers in the field. And yet the Irish government have committed to introducing the Nedap/Powervote system for the whole country at the next general election [10]. This Dutch/British system appears to have been chosen without consulting Irish experts in the field of computer security. Claims by said experts that the system may be insecure are often dismissed as paranoia [11] by both politicians and the public, despite evidence that elected officials do not deserve our unmediated trust.

It is true that an EVS could offer several advantages over manual systems. It could tabulate the results more quickly, eliminate the human error which sometimes occurs in manual vote tabulation, expand the franchise to those currently unable to vote because of special needs, and improve the fairness of the Irish count system.

From a traditional standpoint, however, it is questionable whether or not the Irish electorate needs a faster count. Many active party members have expressed their disappointment that they will no longer be able to enjoy the excitement of a long count. The anticipation involved in waiting for the result is an integral part of our political culture [11].

If the system is going to eliminate human error from counting, it must be developed formally. Human error in the design or implementation of the count software might have considerably more serious, and more far-reaching, effects than human error in the manual system. Formal development is discussed further in the final year project report accompanying this document [12].

Many people with special needs can currently only vote with the aid of an election official, which means that they do not have the same privacy in voting as other citizens. The potential exists to create a system accessible to people with visual, auditory, and movement disabilities.

The form of Proportional Representation (Proportional Representation - Single Transferrable Vote – PR-STV) used in Ireland gives a very accurate representation of the will of the people [13]. Unfortunately, this is at the cost of a very complicated count procedure. One part of the count procedure involves a compromise between efficiency and fairness. Since it is difficult to determine manually which votes should be transferred, votes are taken from the top of the pile – effectively randomly. This does not mean that voting at a particular time makes your vote more likely to be transferred – votes are mixed thoroughly at the beginning of the count process – but it does mean that the late preferences on some votes are given less significance than others. An electronic system could fairly determine which votes should be transferred, removing the need for such a compromise. It is worth noting that this adjustment could only be made to the counting procedures if we make it across the whole system. Which means it could only realistically be introduced once the electronic system was the main medium for vote-casting in the country.

It is a commonly held belief that the change from hand-counted paper ballots to an EVS is inevitable. In that case we must examine carefully what we expect from such a system, and how it should be developed. We must use all the tools at our disposal to ensure that the introduction of an EVS does not put the integrity of our democracy at risk.

Basic Requirements for a Fair Ballot System

"The goal of any voting system is to establish the intent of the voter, and transfer that intent to the vote counter."

– Bruce Schneier, Dec 2000 [14]

Requirements

By developing Mr. Schneier's statement, we can present four stages in voting systems.

- Establish who is "the voter"
- Establish the voter's intent
- Transfer the record of their intent to the vote counter
- Tabulate the result

These stages have a natural order. There is no point in establishing the intent of someone who is not authorised to vote, and we cannot count votes which have not yet been recorded. If each of these stages is to be carried out satisfactorily, certain requirements must be met.

Authenticate

We must begin by establishing who "the voter" is. In most democracies, voting is limited to a particular group (for example, citizens over 18 years of age), each of whom is entitled to vote once. To prevent personation[1], we must establish the identity of people attempting to vote. If someone is successfully identified as eligible we must record that they have been given their opportunity to vote and we must then give them that opportunity.

Establish Voter Intent

If we are to establish the voter's own intent, we must prevent voter coercion and verifiable vote sale. We protect the voter's privacy so that no-one else can verify whether they voted the way they were instructed. As stated above, the voter's identity must be recorded so that each voter can vote only once. Their vote, of course, must also be recorded. In order to prevent conflict between these two requirements we must record the vote and identity separately, while ensuring that a vote is only ever recorded for someone who has been successfully identified as eligible.

[1] Curiously, personation is the correct term for impersonation with intent to fraud.

We must also ensure that the interface is adequately usable to give the voter a fair chance of recording their vote correctly. It is impossible to develop an interface which can never be misunderstood but there are heuristics available to the interface designer [15]. These include using designs already familiar to the user, and using metaphors which make the interface more intuitive.

Transfer the Vote

The vote must be transferred from the voter to the vote counter. It is important that the vote cannot be altered or removed at this stage, for obvious reasons.

Tabulate the Result

We use the word “tabulate” here, rather than “count” because count really doesn’t convey the complexity of the task, especially for the Irish PR-STV system [13]. Apart from the obvious requirement that the votes be tabulated correctly, it is vital that the votes are seen to be tabulated correctly. A voting system is only as good as the public believe it to be. It must, therefore, be possible to independently re-tabulate the results. This last requirement also extends over all the other requirements. The public cannot be sure that the correct result was tabulated if they are not sure that, for example, all votes were recorded correctly.

Summary

We note that these requirements are not from the point of view of individual voters, who might prefer to be able to prove how they voted. They are, rather, from the point of view of the people as a whole. These are the requirements which must be met in order to ensure that the representatives elected are the representatives chosen by the people.

To summarise (and please note that order does not indicate priority):

1. the system must allow only eligible voters to vote, and they must be allowed to vote only once,
2. the voter’s identity and their vote must be kept separate,
3. the voter’s intent must be recorded correctly,
4. the vote cannot be altered or removed once it has been recorded,
5. tabulation must be accurate and independently reproducible, and
6. the public must be confident that all the above requirements are met.

No voting system can perfectly meet all the above requirements, but they must be met at least enough to ensure that fraud is not occurring on a wide enough scale to alter the result of an election.

Manual System

In the Irish paper ballot system, the voter goes to the polling station where their vote is registered. If they are successfully authenticated, they are marked off the register and at the same time given a valid ballot paper, fulfilling requirement 1. These ‘Australian ballots’ are pre-printed and bear some distinctive markings that ensure that valid papers are easily distinguishable from invalid papers. The voter then indicates their choice and deposits the paper in a ballot box.

Requirement 2 is achieved with the use of a ballot paper and ballot box. The ballot paper acts as a kind of token indicating that the holder has been authenticated, but which gives no clue as to their identity. The ballot box ensures that the voter’s paper cannot be viewed by anyone other than the voter himself.

Requirement 3 is met by providing a paper with a simple and familiar interface. During the vote collection phase, ballot boxes are at all times visible to polling station staff and interested observers. Their transport is supervised by members of the Garda Síochana and representatives of running candidates – or sides, in a referendum. This means that requirement 4 is fulfilled because any manipulation of the ballots would be detected. The tabulation process involves many people, again being supervised closely.

The ballots are retained so that they can be used in recounts. The combination of the two fulfills requirement 5.

The sixth and final requirement is fulfilled, again by the fact that the whole process is supervised. The familiarity of the electorate with the system, and their belief that it has worked up until now also contribute to their confidence.

Remote Electronic Voting

"A secure Internet voting system is theoretically possible, but it would be the first secure networked application ever created *in the history of computers.*"
– Bruce Schneier, Dec 2000 [14]

Remote electronic voting (REV) refers to any system where the user does not have to be in a polling station in order to register their choice. The most common proposals for REV envisage voting via the Internet. But other media, such as mobile phones, are being considered by the British government and the European project eucybervote [16, 17].

Technological Problems with REV

Separating Vote and Voter

REV systems must meet the same requirements as any other voting system. They must authenticate voters, store their identity, and collect their vote. This is where the problem of separating voter identity from vote arises. As Dr. Rebecca Mercuri and Bruce Schneier have both pointed out [1, 18], voting is different from other secure transactions made on the Internet. For example, financial transactions via the Internet rely on a model where the identities of all parties are provably linked to the transactions themselves. This allows for re-validation of the transactions should their validity be called into question at a later date. Clearly this model is not suitable in the case of electronic voting. We must accept votes only from successfully authenticated voters, but we cannot attach the voter's identity to the vote to prove later that it came from an authenticated voter. As Dr. Mercuri says:

> "...the privacy constraint directly conflicts with the ability to audit the ballot data." [1]

Secure Connection

Even if we could surmount this problem by developing a new model of computer security, there are other difficulties associated with remote vote collection. The voter's identity must be transferred from their device to the authentication server, followed by their vote. This must be done securely. We cannot allow malicious observers to view the voter's identity and vote (requirement 2), nor can we allow the vote to be altered or prevented from reaching its destination (requirement 4).

The connection between the voting device and the authentication server must be secured, and in practical terms this means using encryption. This is particularly true of the Internet, where it is very simple to observe – and interfere with – other people's traffic, but it is also true of other media. Individuals or groups with an interest in affecting the result of an election, or in knowing how individual voters vote, may well have the resources to tap into phone lines – land or mobile – or the technology to view SMS text messages. However, strong encryption requires knowledgeable users, since one of the weakest parts of any cryptosystem is key management [19]. The greater mass of voters cannot be expected to manage encryption keys responsibly, so it is likely that any cryptosystem used in an REV system would have to trade security for usability.

Viruses and DoS Attacks

Peter Neumann [20] says:

> "...the Internet is not safe for elections, due to its vast potential for disruption by viruses, denial-of-service flooding, spoofing, and other commonplace malicious interventions."

(quoted in Dr. Rebecca Mercuri's paper "a Better Ballot Box?" [1])

We have to assume that the majority of voters are relatively uninformed computer users running unpatched and virus prone installations of Microsoft Windows on an Intel machine [8]. It would be easy, then, for hostile parties to develop a computer virus to affect the result of an election. Such a virus could easily be disseminated to the majority of voters, and if it was designed to have no effect except on voting software, might never be detected. Douglas Jones suggests a design for a virus which could affect the outcome of an election [21]. This virus would alter the voting-interface of a small number of voters. The number is chosen to be large enough to have an effect, but not large enough to be obvious. The altered interface would lead the voter to believe that they had voted for the most popular candidate, when they had actually voted for the candidate supported by the author of the virus. Other types of viruses might send the voter's details along with their vote to some server, or simply prevent them from voting.

The vote server itself would be in danger of attack. Denial of Service (DoS) attacks are easy to launch, and can force a server off the network. In 2000 Yahoo was brought down by a DoS attack [22]. If any hostile individuals or groups wished to disrupt or halt the election, launching a successful DoS attack on an election server would serve their purposes well.

Security experts are generally in agreement that remote electronic voting is not safe [14, 23, 24].

Sociological Problems with REV

Apart from the technological problems we have already discussed, mention must be made of the sociological problems.

Remote voting requires technology. All such technology costs money. In 2001, only 25% of the Irish population were using the Internet [25]. If remote voting were to become the dominant form of voting, it could result in an increased disenfranchisement of the poor [26].

One key feature of the polling station is the voting booth. This is the area where a voter goes to mark their ballot paper before depositing it in the ballot box. No-one is allowed to enter the voting booth with the voter (barring certain circumstances, like special needs). This provides security against two important dangers to the integrity of the voting system – voter coercion and verifiable vote sale. When a voter enters the voting booth, they are alone and unwatched. No-one can force them to vote in a particular way. Similarly, anyone who paid a voter to make a particular choice would have no guarantee that their investment had paid off. This is not to say that voter coercion and vote sale do not occur in Ireland today – they almost certainly do. But thanks in part to the voting booth, they are kept to an acceptable minimum. By its very nature, remote electronic voting prevents us from even approximating the safeguard provided by the voting booth.

Kiosk Voting

"...I will continue to urge municipalities to ONLY consider the purchase of voting systems that include a voter-verified physical audit trail. These systems would include mark-sense (or optically scanned) paper ballots, or kiosks that produce a paper receipt that the voter can review and must drop in a box for recount ... "
– Dr. Rebecca Mercuri [23]

Kiosk voting is the most descriptive term commonly used for electronic voting systems in which the voter must go to some sort of polling station in order to register their vote. It is spared the remote authentication problems which plague remote electronic voting, because the authentication and vote collection processes can be kept completely separate, connected only by some token which authenticated voters receive, and which entitles them to vote. It is recommended that the existing manual authentication process used in Ireland – which would not particularly benefit from automation – be used in conjunction with any EVS introduced here. Requirements 1 (authentication) and 2 (privacy) are thus met in the same way as they are in the paper system. The only difference is that the ballot paper would be replaced by some similarly difficult to reproduce token which would entitle the holder to use the voting machine.

The Mercuri Method

Over a decade ago, Dr. Rebecca Mercuri proposed the Mercuri Method, the use of which would result in an EVS that met all our other requirements at least as well as the paper system does. She describes the method as follows:

> "…the Mercuri Method, requires that the voting system print a paper ballot containing the selections made on the computer. This ballot is then examined for correctness by the voter through a glass or screen, and deposited mechanically into a ballot box, eliminating the chance of accidental removal from the premises. If, for some reason, the paper does not match the intended choices on the computer, a poll worker can be shown the problem, the ballot can be voided, and another opportunity to vote provided." [1]

The EVS could tabulate the results very quickly from its records, but if there was any doubt about its results, the paper ballots would be considered the official votes. It would be reasonable to implement a system of spot-checks – where randomly chosen constituencies would have their paper ballots counted and compared to the electronic result – for the sake of public confidence. This is the method endorsed by computer security expert and cryptographer, Bruce Schneier [14].

Other Measures

However, in the general case, the electronic result would be taken as correct. We should try, therefore, to ensure that the system itself, without the paper record, meets our requirements.

We must ensure, for the sake of requirement 2 (voter privacy), that the EVS will not provide information about the order in which votes were registered. An observer in the polling station could make note of the order in which voters entered the booth, and if the votes were recorded in chronological order they might then be able to figure out how individual voters voted. Technology such as a combination of pseudo-random number generation and a hashing algorithm might be used for this purpose.

We cannot be sure that a voter's intent is being recorded correctly within a completely electronic system (requirement 3). However, a user interface that is skillfully designed should improve the voter's chances of transferring their intent into the system. When marking their preferences on paper ballots, voters sometimes give the same preference to more than one candidate, or skip a preference (for example marking preferences 1, 2 and 4). An EVS might prevent the voter from making such mistakes – by only giving the voter two options: marking their next available preference or revising their current preferences – or it might alert them to their mistakes, and give them the option of revising. This facility cannot be offered by the manual system without threatening the voter's privacy.

If we assume that the vote has been recorded correctly, we can ensure that it cannot be altered or removed (requirement 4) by storing the votes in a medium that can be written to only once.

If the count software is developed formally, we can be reasonably sure that the votes are tabulated correctly. This topic is discussed in greater detail in the final year project report accompanying this paper [12].

The second part of requirement 5 is that the results can be reproduced independently. To do this we must refer to the printed ballots – it is unlikely that an incorrect electronic tabulation of the votes would be highlighted by rerunning the tabulation software. As mentioned above, the result of a count can be affected by which ballots are chosen for transferral. So in order to independently reproduce the same results we must transfer exactly the same ballots that were transferred in the electronic tabulation. This requires that we print some information the ballot which links it to the relevant record within the EVS.

And finally requirement 6 – public confidence. Unfortunately, public confidence in the system appears to be a requirement all too easily met. As will be discussed in the next section, the Nedap/Powervote system does not appear to deserve this confidence. However, any security expert who is not convinced of the system's security might be able to shake the public's confidence. Such experts could be made more confident if formal methods [27] were used in the development of the system, and if all source code and specifications were publicly available.

It is the computer science community who have the expertise to recognise security flaws in an EVS. Any EVS introduced in Ireland ought to convince the computer science community that it is safe. Otherwise, they will be responsible for convincing the general electorate that the system is – or could be – unsafe.

It should be noted that these measures are adequate only when combined with the Mercuri Method. We cannot be fully sure that an electronic voting system without ballot paper backup is not displaying one thing to the voter as their vote, whilst recording something entirely different. These measures when properly in place, however, do make the EVS reliable enough to be worth using as long as we have the paper record. An EVS which does not implement these measures may be vulnerable to attack from opponents of electronic voting. If they could make the electronic results differ from the paper results, they could eliminate the use of electronic voting.

Case study: Nedap/Powervote

There are many voting systems in existence that could have been chosen for this case study, but the one of greatest relevance in Ireland is the system recently adopted by the Irish government.

The Nedap/Powervote system utilises the existing manual authentication process to fulfill requirements 1 and 2 – voter authentication and privacy – as recommended. The rest of the Nedap system is less satisfactory, however.

In March 2002 the Department of the Environment and Local Government (DoELG) requested that Zerflow [28] carry out a security assessment of the Nedap/Powervote voting machines. The Zerflow report [29] which we obtained under the Freedom of Information Act [30] highlights some serious security flaws in the system. The report has not been published, and its findings have been lightly dismissed by the DoELG [31]. The minister's statement that

> "The concerns raised by the Zerflow report were fully assessed by the Department and the machine manufacturers." [31]

is not reassuring. The DoELG presumably have little expertise in the area of computer security, and the manufacturers are unlikely to agree that their system has flaws.

According to the Zerflow report, the interface can be tampered with. In response, the minister has stated that

> "...the present cover used for the machine ballot paper is considered adequate." [31]

The training guide for polling station staff [32] recommends that staff "occasionally check that the ballot paper/screen has not been interfered with." There is no indication of what will happen if it has been interfered with, and if votes may be compromised.

The second major problem identified by Zerflow is that the backup cartridge is left in the voting machine after polls close. There is a danger that the backup will be altered or wiped while still in the machine. If the primary cartridge is unusable for some reason, it is vital that the backup cartridge has been kept secure.

The very fact that the voting machine has the capability to wipe the contents of the backup cartridge is worrying. Such features should be isolated from publicly accessible parts of the system. If the system contains such obviously bad design decisions, what else might it contain?

Zerflow also report that the key which gives polling station staff access to sensitive features on the machine is easily copied, and can be ordered by serial number. The training guide recommends that

> "If there is an occasion (emergency) when the Control Unit is unattended remove the key from the unit and give it to the Presiding Officer." [32]

It is easy to conceive of a scenario where a hostile person or group has acquired a key, and creates a diversion so that they can gain access to the machine for 5 minutes.

Although the interface rated highly in an MBRI survey quoted in [33], gaining a mean rating of approximately 3.77 out of 4 overall, it is difficult to gauge the accuracy of this survey, as neither the questions nor the detailed results are available. Quoted in the same document, however, are a selection of the more unfavourable comments, and some of them appear to be quite serious, for example:

- "Too dark/numbers didn't light up",
- "Display/names/photographs too small", and
- "Numbers too small". [33]

Since the system does not print out the vote for the voter's examination, we have no guarantee that votes are recorded correctly. To quote Dr. Rebecca Mercuri:

> "Any programmer can write code that displays one thing on a screen, records something else, and prints yet another result. There is no known way to ensure that this is not happening inside of a voting system." [34]

The source code for the system is not publicly available. In fact, even the government do not have a copy. If someone were interested in affecting the outcome of Irish elections, they might compromise one of the programmers within Nedap, or manage to have someone employed there. Skilled programmers could insert changes which could affect the outcome of an election, whilst being very difficult to detect. Opening the source to the general public would make it much more likely that such changes would be detected.

All of these things do not necessarily add up to an immediate danger. But even if no malicious person or group tried to exploit the flaws mentioned, these flaws do have certain implications about the standard of design and implementation that went into the creation of the system. PR-STV is a complicated system, and it is perfectly realistic to assume that some mistakes may have been made in the development of the count software, especially since the system was not developed formally. There is no need for malicious attack on the system; human error in the voting machine or count software might be enough to give the wrong result.

Conclusion

"...how many developing nations would trust their governments or unknown individuals in generally unknown companies to conduct an election electronically?"
– Karlin Lillington, Oct 2002 [35]

If a kiosk voting system were developed according to the principles outlined here, it could offer several advantages over the manual system. Voters could be offered the opportunity to correct any mistakes. Tabulation would be faster and more accurate, and could be made fairer and more people could be given the chance to vote. Such a system is theoretically possible, but the Nedap/Powervote system does not reach a satisfactory standard.

The introduction of electronic voting in Ireland, in its current form, threatens the integrity of our democracy. As demonstrated in this report, this is an issue that has been incompetently addressed by the government. The cost of the development of a suitable system, and whether the potential advantages would justify that cost, remain undiscussed. It is clear that it is the responsibility of the computer science community in Ireland to assess the system being introduced, and to make itself heard [35].

References

[1] Dr. Rebecca Mercuri. A Better Ballot Box? *IEEE Spectrum Online*, October 2002.

[2] Making it Easier to Vote - Electronic Voting and Counting.
http://www.environ.ie/elecvote_detail.pdf.

[3] Nedap home page.
http://www.nedap.nl/company/item_company.html.

[4] Government papers about electronic voting.
http://www.environ.ie/elections/Elect_Voting_Roadshows.pdf,
http://www.environ.ie/elections/Elect_Voting_Answers1.pdf,
http://www.environ.ie/elections/Elect_Voting_Answers2.pdf,
http://www.environ.ie/elections/Elect_Voting_Info_Paper.pdf.

[5] Cynthia Farrar. *The Origins of Democratic Thinking - The invention of politics in classical Athens*. Cambridge University Press, 1988.

[6] *The Concise Oxford Dictionary of English Etymology*. Oxford University Press, 1996.

[7] Peter Singer. *Democracy and Disobedience*. Gregg Revivals, 1973.

[8] Aviel D. Rubin. Security Considerations for Remore Electronic Voting. *Communications of the ACM*, 45(12), December 2002.

[9] Dr. Rebecca Mercuri. Florida 2002: Sluggish Systems, Vanishing Votes. *Communications of the ACM*, 45(11), November 2002.

[10] Political Correspondent Mark Brennock. All constituencies to have electronic voting in 2004. *The Irish Times*, Thursday, October 31st 2002.

[11] Dan White. The real price of electronic voting. *Irish Computer*, 26(10), November 2002.

[12] Margaret McGaley. Electronic Voting: A Safety Critical System. Final Year Project Report, NUI Maynooth Department of Computer Science 2003.

[13] Cornelius O'Leary. *Irish elections, 1918-77 : parties, voters, and proportional representation*. Gill and Macmillan, 1979.

[14] Bruce Schneier. Voting and Technology.
http://www.counterpane.com/crypto-gram-0012.html#1.

[15] Kevin Cox; David Walker. *User-interface Design*. Prentice Hall, 1993.

[16] e-Voting Security Study. *http://www.edemocracy.gov.uk/library/papers/study.pdf*. 2002 Crown Copyright.

[17] CyberVote. *http://www.eucybervote.org*.

[18] Bruce Schneier. Internet Voting vs. Large-Value e-Commerce.
http://www.counterpane.com/crypto-gram-0102.html#10.

[19] Key Management Guideline. *http://csrc.nist.gov/encryption/kms/guideline-1.pdf*.

[20] Peter G. Neumann's Homepage. *http://www.csl.sri.com/users/neumann/*.

[21] Douglas W. Jones. Trustworthy Systems on Untrusted Machines. *http://www.cs.uiowa.edu/˜jones/voting/atlanta/*, June 2002.

[22] Robert Morris, Frans Kaashoek, Hari Balakrishnan, and Students MIT LCS. *http://www.pdos.lcs.mit.edu/˜rtm/slides/jason1.ppt*.

[23] Dr. Rebecca Mercuri's website on electronic voting. *http://www.notablesoftware.com/evote.html*.

[24] Peter G. Neumann. Security Criteria for Electronic Voting. *http://www.csl.sri.com/users/neumann/ncs93.html*, September 1993.

[25] Susan O'Donnell. The Internet in Ireland: Patterns of consumer use, projections for future use, and implications for the public sphere. *http://www.models-research.ie/publications/art/01-5d.html*, 2001. Paper presented to the Digital Landscapes: Media Transformations in Ireland symposium, Dublin Institute of Technology, 18-19 May.

[26] SecurePoll Electronic Voting Update: Mar 09 2000 - Mar 19 2000. *http://www.securepoll.com/Archives/Archive3.htm*.

[27] Andrew Harry. *Formal Methods Fact File : VDM and Z*. Wiley, 1996.

[28] Zerflow homepage. *http://www.zerflow.com/*.

[29] Zerflow Report. Available from the Department of the Environment and Local Government under the Freedom of Information Act 1997.

[30] Freedom of Information Act, 1997. Available online at the website of the office of the Attorney General *http://www.irishstatutebook.ie/1997_13.html*.

[31] Electronic Voting System. website. Dáil Debate - Tuesday, 10 December 2002.

[32] Polling Staff Training Guide. Institute of Public Administration, obtained from polling station staff.

[33] Electronic Voting and Counting. InformationOnElectronicVoting2.doc. Document received from Mr. William Stapleton of the Franchise section of the DoELG.

[34] Dr. Rebecca Mercuri. Dr. Rebecca Mercuri's Statement on Electronic Voting. *http://www.notablesoftware.com/RMstatement.html*, 2001.

[35] Karlin Lillington. Electronic vote poses big security risk. *The Irish Times*, Friday, October 18th 2002.