AN ROINN COMHSHAOIL AGUS RIALTAIS ÁITIÚIL

DEPARTMENT OF THE ENVIRONMENT
AND LOCAL GOVERNMENT

Dear Mr. Boon,

Further to your e-mail to Mr. Murphy please find herewith
a copy of the Zerflow report on voting machine security
together with the Minister's response to the issues raised
therein.

Yours sincerely,

M. Gleeson

Freudin Staton.

Website: www.environ.ie

Adjournment Debate - 10 December 2002

"The reported deficiencies in the electronic voting system as outlined in the Zerflow Report and the need to have the report published in full."

Deputy B Allen.

This matter has attracted a considerable amount of media coverage in the last few days and I welcome the opportunity to bring some balance to that reporting and to reassure Deputies that the electronic voting system is accurate, reliable and secure.

From the outset, security has been paramount in the design, testing and implementation of the new system. The testing programme, in particular, has been rigorous: the voting machine has been tested by two international test institutes PTB in Germany and TNO in the Netherlands, both of whom have certified the machine as suitable for use.

Zerflow, an information security company, was requested by my Department in March 2002 to carry out a further security assessment of the procedures to be applied in the use of voting machines in the physical environment of polling stations. This was a subsidiary and less extensive exercise than the other tests to which I have referred; and it was carried out at a cost of some €4,000 plus VAT over 14 days.

The report was received on 27 March 2002 and it contained 16 recommendations. A small number of these were embodied in my Department's subsequent instructions to returning officers.

An analysis of the report's main recommendations however revealed an inadequate understanding of the organisation of election preparations, including arrangements in polling stations.

The concerns raised by the Zerflow report were fully assessed by the Department and the machine manufacturers. They were not considered to present any realistic threat to the security of the voting process, having regard to the design of the machine and to security arrangements operating in polling stations.

It was also relevant to this assessment that similar machines (but incorporating fewer security features) are used extensively in Germany and the Netherlands. The concerns raised by Zerflow have not been identified in risk assessments in these countries.

As most of the focus of media attention has been directed to the first recommendation in the report, I would like to deal with it. It contained 3 parts as follows –

- that a perspex or glass cover should be placed over the ballot paper and the cover should be secured and alarmed;

- that regular checks should be made to ensure nobody defaced or interfered with the surface of the protective glass; and

- that regular checks should be made to ensure that the voting buttons represent the correct candidates and that candidate information is correct.

The latter 2 items have in fact been addressed in my Department's instructions to returning officers.

As regards the first item, the present cover used for the machine ballot paper is considered adequate. It is not accepted that the ballot paper can be easily interfered with. The security arrangements in polling stations involve the deployment of a poll clerk full time to supervise the use of each voting machine. Given the highly intrusive operations which would be necessary to remove the ballot paper cover from the machine, interference of the kind suggested could not occur without active collusion of polling station staff. The well supervised and honest administration of polling stations, under the authority of returning officers, is a key prerequisite for the good conduct of elections in Ireland in relation both to manual and electronic voting.

My Department's conclusion therefore was that the main scenarios identified by Zerflow were implausible, and that the probability of their occurrence without detection was so remote as to be properly discountable.
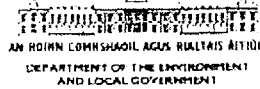
Electronic voting is rightly seen as a progressive and welcome modernisation of our electoral process. I acknowledge that it is integral to the acceptability of the new

system that there should be confidence in its security, as well as in its greater accuracy and efficiency.

Deputies should also bear in mind that the electronic voting machines in their present form will all be replaced at the 2004 elections by new or upgraded machines. As part of the process of acquiring and commissioning these machines, we will of course look again at security issues.

information security

Zerflow

**Electronic Voting
Security Assessment
For**

AN ROINN COMHSHAOIL AGUS RIALTAIS ÁITIÚIL
DEPARTMENT OF THE ENVIRONMENT
AND LOCAL GOVERNMENT

Franchise

Originator   :   **Colin English**

Approval   :   **Tony Geraghty**

Date Approved   :   **27/03/2002**

**Zerflow
Arena House
Arena Road
Sandyford
Dublin 18
Rep of Ireland**

**Tel: +353 (0) 1 293 0155
Fax: +353 (0) 1 293 0156**

CONTENTS

THIS DOCUMENT CONTAINS 19 PAGES INCLUDING HEADER PAGE

Disclaimer

The information contained within this Report is the property of Zerflow Holdings Ltd. and is issued in confidence and must not be reproduced in whole or in part or used in tendering or manufacturing purposes or given or communicated to any third party without the prior written consent of Zerflow Holdings Ltd.

This Report does not form or constitute part of a contractual document, nor does its submission imply acceptance of any commercial terms.

No advice given or statements or recommendations made shall in any circumstances constitute or be deemed to constitute a warranty by Zerflow Holdings as to the accuracy of such advice, statements, or recommendations. Zerflow Holdings shall not be liable for any loss, expense, damage, or claim arising out of the advice given or not given or statements made or omitted to be made in connection with this report.

1 Background

The Government is to phase in an electronic voting system that will make a significant change to the traditional electoral process. The new system will also mean the end of marathon vote counts by hand. At the last general election in 1997 it took more than a week to decide the result in Dublin South East.

Future ballot papers will feature pictures of candidates beside their party emblems, where applicable, and voters will press a button to make their choices under the proportional representation electoral system.

At present, counting does not begin until the day after elections and takes an average of about 12 hours to complete nationwide. The machines to be used, provided by a Dutch company, will be tested over the next six months and will be used for the first time in a selected number of constituencies at the next general election.

Zerflow have been engaged to examine the voting machine to be used by voters and make comments on any security weaknesses found.

2 Introduction

Department of Environment has requested Zerflow to outline the components of a Security
Assessment of the Electronic voting system. Those components include the following:

- The Voting machine.
- Data cartridge.
- Control Consol.
- Any peripheral devices attached to the machine or in its surrounds, critical to its
  function.

This document outlines the security weaknesses discovered by Zerflow staff during the
review. The security review was focused only on the voting machine, the control console and
the data cartridge. The procedures and policies surrounding the implementation and use of
the voting machine were also examined as part of the review.

3 Scope

The following sections outline the scope of work for a security assessment.

3.1 Risk Analysis

Threats facing Electronic voting could include anything from human error to malice, to organised corruption of the voting process. How do you decide which ones are a realistic problem? How can you effectively manage these risks? Zerflow will apply risk analysis to bridge the gap between risk and technology.

In addition we will:

- ◆ Define what we are protecting.
- ◆ Analyse the voting machine to identify technical vulnerabilities.
- ◆ Consider the effects of a breach in security and what happens if a breach occurs.

3.2 Technical Assessment

Zerflow will carry out a comprehensive assessment of the physical hardware, its applications, and its data storage devices. This assessment will measure the system from the following critical viewpoints:

- ◆ Availability
- ◆ Integrity
- ◆ Usability
- ◆ Confidentiality
- ◆ Authentication

3.3 Policy Assessment

Review of the Security and Operational policy: - critical evaluation and benchmark evaluation to include the following:

- ◆ Security Organisation
- ◆ Asset classification and control
- ◆ Personnel security
- ◆ Communications and operational management
- ◆ Physical security
- ◆ Systems access control
- ◆ Data Access, Distribution and Storage
- ◆ Process continuity and redundancy planning

The Policy is of utmost importance, because the bedrock of security is based on defined, repeatable processes, which are constantly enforced. Zerflow uses ISO17799, the international standard for Information security to benchmark Security policy.

3.4 Process Assessment

Review of the entire process, establishing the critical points, identifying their level of vulnerability and determining how you respond if those resources are compromised, or failure occurs.

A thorough testing of each atomic stage of the process will be carried out to encompass the following (where practicable):

- Usability test
- Stress test
- Functionality test
- Error test
- Availability test
- Confidentiality test
- Process-abandoned / aborted test
- Failure test
- Integrity test

4   Interim Report

Zerflow highlighted the following issues at a meeting with Peter Green. These issues arose from a discussion between Zerflow staff with little knowledge of the voting machine. It was after this meeting that Zerflow were requested to conduct a full review of the voting machine.

4.1 Immediate issues of concern

1. What actions and processes are audited, how is the audit trail linked, and who has access to that audit?

2. In the case of dispute, is there any sort of recount, or manual input via audit trail?

3. What facility is provided so that a voter can only vote in the allowed votes (e.g. A U.S. national cannot vote in Dail election, but can vote in local election)? If two polls held on same day, what stops this person voting in the Dail election?

4. How does the system confirm that each vote has been accepted (or rejected) and recorded?

5. If the system fails, what is in place to cope (e.g. electricity failure/ power surge)? If the system is inoperable, what system takes place?

6. If the system fails during the days polling, and an alternative system is used, how are the two systems reconciled, and tabulated?

7. How does the local poll centre staff know, and verify that the system is working correctly?

8. If the system does fail, and an alternative system used, how is a guarantee given that the system is no longer operable by unauthorised persons?

9. What is the fault tolerance, and how has it been validated?

10. In the case of a dispute (e.g. at the count centre it transpires that a candidate expected to poll approx 7,000 first preference votes only gets 300, and a candidate normally expected to get approx. 300 votes, gets 7,000 votes. There has clearly been an error, and the candidates' details and recorded votes have been mixed up): does that election stand, is there a method of checking, can the audit trail provide any further information?

4.2 Scenario

In the case of point 10:

Fraud had been planned by an organised group of people. They have got access to the card that is placed on to the electronic voting console, and have reprinted the card, but switching their preferred candidates place with a much more popular candidate, and visa versa. Very early in the polling day, they send out a team to switch the genuine card with the fraudulent card, and again towards the end of the day, they switch the cards back.

People voting all day give the number one to the button indicated by the candidates' details, but are in fact casting votes for the wrong candidate. Whilst the plan works, at the count centre fraud is suspected by the massive disparity in votes to those expected.

In the above case, what procedures are put in place to prevent this occurrence in the first place? Should it occur, what procedures are in place to detect and rectify it during the polling day? Should it go undetected, what is in place to correct, or indeed nullify the result on counting day?

5   Executive Summary

The government are introducing a new electronic voting system to replace the paper ballot system. Voters will now use buttons beside electoral candidates to cast their votes. The electronic system will remove the arduous task of vote counting and also the need for recounts.

Although electronic voting is both labour saving and efficient, this opens the election to new scepticism from the public. Can this new system be trusted to deliver the correct results? Can hackers tamper with this new system? These are all questions that Zerflow endeavoured to answer during this review.

Zerflow were engaged by Peter Green to analyse the voting machine from a security perspective. Other parties have previously carried out a full code review and numerous other tests. Zerflow's objective in this project was to find weaknesses in the policies, procedures and the physical security of the voting machine that may be exploited to compromise an election.

Zerflow identified several high level vulnerabilities that should be addressed as soon as possible to enhance the overall security of the project. The integrity of the ballot sheet cannot be guaranteed with the current equipment and controls. As demonstrated in the case study above, voters can easily be duped into voting for the wrong candidates by simply taping a fake ballot to the front panel of the voting machine. Our tests also revealed that the front panel is only secured by one switch that can easily be used to open the panel and access the ballot card.

Zerflow recommend that the ballot card be protected by a glass or Perspex cover with holes to allow access to the voting buttons. Zerflow also recommend that a procedure is implemented which will have the control panel operator regularly check the ballot card and ensure that the voting buttons represent the correct candidate.

Zerflow also recommend securing both the front and back panels on the voting machine and also alarming these panels to prevent unauthorised access.

Zerflow identified another high level vulnerability associated with the key used in the control console. Zerflow were able to get a copy of the control console key made at a local shopping centre. Anybody with access to this key could potentially cast votes on a voting machine. This key could also have been ordered using the serial number on the key.

Zerflow recommend the use of 2-factor security for the control console. This type of security would require the presiding officer to have a smart card and a personal PIN number. Even if somebody got access to the smart card, they would still need to PIN to be able to vote.

Due to time constraints, 2-factor security may not be implemented before the election. A compromise would be to separate the keys from the control consoles and send them

separately to the polling station in secure sealed packages. The keys should also be returned with the cartridges and stored in a secure location.

During the review it became apparent that the backup cartridge remains in the voting machine after the poll has been closed. If the main cartridge were to be damaged then the backup cartridge will be required to complete the count. For this reason the backup cartridge should be removed from the voting machine and treated as securely as the main cartridge. A further check would be to use one count machine for the main cartridges and another for the backup cartridges at the count centre. Both counts should return with the same result.

The 'Technical Summary' contains a more detailed listing of the issues uncovered during the review.

6   Technical Summary

This section of the report contains detailed findings from this security review.

6.1   Findings and recommendations

Zerflow has identified several issues during this review. These issues are listed in order of priority. The high level issues should be addressed as soon as possible as these issues could cast doubt over the integrity of an election using the voting machine.

HIGH LEVEL ISSUES
◆   The front cover of the voting machine can be easily tampered with. This could allow somebody to interfere with the ballot card and cause voters to select the wrong candidates. This action could very easily go unnoticed and compromise the entire election in that constituency. Zerflow recommend that a Perspex or glass cover is placed over the ballot card and that this cover is secured and alarmed on the voting machine. This cover will need to be crafted specifically with holes to allow users to access voting buttons. Regular checks will also be required to ensure that nobody has defaced or interfered with the surface of the protective glass. These checks should be carried out regularly after a specified number of votes. Checks should also be carried out regularly to ensure that the voting buttons represent the correct candidates and that all candidate information is correct. All of these checks should be logged to prove that there has been no interference with votes.
◆   The key used to operate the control console is not secure. Zerflow were able to get a copy of the control console key made at a local shopping centre. Anybody with access to this key could potentially cast votes on a voting machine. This key could also have been ordered using the serial number on the key. Zerflow recommend the use of 2-factor security for the control console. .This type of security would require the presiding officer to have a smart card and a personal PIN number. Even if somebody got access to the smart card, they would still need to PIN to be able to vote. Due to time constraints, 2-factor security may not be implemented before the forthcoming election. A compromise would be to separate the keys from the control consoles and send them separately to the polling station in secure sealed packages. The keys should also be returned with the cartridges and stored in a secure location.

◆ In the event of a power loss, unless the control unit operator is keeping a constant count of votes there will be no way of knowing if a voter has actually cast a vote.

If a power outage affected a voting machine, this problem could potentially allow a voter to vote twice.

The voting machine should have a feature which will indicate to the control unit operator if a vote was not cast while in voting mode before the power outage. The control unit operator could then recall that voter and permit a vote.

◆ The rear cover for the voting machine should be made of metal and alarmed to prevent access to the cartridges.

At present the rear cover of the voting machine is made of plastic and provides no security for the internal computer and the voting cartridges.

The internal computer and the cartridges must be secure at all times. The rear cover should be made of metal and alarmed.

◆ Backup cartridges remain in the voting machine.

Back cartridges remain in the voting machine after an election when the main cartridges are removed. If a backup cartridge were required because of damage to the main cartridge or failure, the integrity of information on the backup cannot be trusted.

The backup cartridge should be secured in the same way as the main cartridge.

◆ Backup cartridges can be wiped in the voting machine.

The backup cartridge can be wiped on the voting machine.

The voting machine should not be able to wipe the backup cartridge. This operation should only be possible on the programming unit.

MEDIUM LEVEL ISSUES

- ◆ The voting machine should be powered off when accessing the cartridge or changing the paper.

If the internal computer in the voting machine is being accessed while the power is on, this could cause damage to the voting machine, the data cartridge or cause personal injury to an operator.

Electrostatic protection should also be used when accessing the internal computer and removing the cartridges.

- ◆ Storage of cartridges after counting.

The cartridges must be stored in a suitable location for the period required by legislation.

- ◆ The voting machine needs to be secured to a table by some means.

At present the voting machine requires a separate stand or table. The voting machine could be easily pushed off this table and damaged beyond repair, or cause personal injury to the control unit operator.

Zerflow recommend that the voting machine be secured to a table when in use. If it is not possible to implement this measure before the election, then the voting machine should have rubber feet attached to the base to prevent accidental damage.

- ◆ The voting machine does not display a CE compliance sticker.

The CE Marking regime requires companies to ensure that their products comply with the mandatory health and safety requirements spelled out in EU directives. For more information on CE, see Appendix B.

The voting machine has a number of visible wires around the front panel light area. A CE audit would determine if situations like this are dangerous. Zerflow recommend that the manufacturers get a CE audit and implement any changes required.

LOW LEVEL ISSUES

◆ The data stored on the cartridges in not encrypted.

The data stored on the cartridges is stored in clear text and could potentially be changed. This is highly unlikely in the short term, but as the voting machines are used more in the future, people's awareness to the process and hardware will also increase. Encryption will aid in maintaining the integrity of information.

The data on the cartridges should be encrypted and check summed to help guarantee the integrity of the information.

◆ The voting machine can only support a maximum of 56 candidates for a single election.

This limit of candidates could easily be exceeded to prevent the use of the voting machine. Under recent legislation (ELECTORAL (AMENDMENT) BILL, 2002) 30 signatures are required to register a candidate. The monetary deposit requirement has also been removed. Any group could potentially register candidates just to prevent the use of the voting machine in one or all constituencies. With 16 candidates in Meath in the last election, a 56 candidate limit may be low.

Zerflow recommend that this problem addressed as soon as possible.

◆ There may be an issue with voting machine availability during peak hours.

Many voters using the voting machine may not be computer literate and spend longer voting that they would on a paper ballet. This may cause problems during peak voting hours.

Zerflow recommend that consideration be given to the number of machines required to cope with large numbers of people waiting to vote, especially at peak times.

◆ The pictures of candidates and party symbols on the ballot paper are small and of bad quality.

The pictures on the ballot sheet are small and of bad quality.

Zerflow recommend reviewing the size of the pictures used and enhancing the quality of these pictures by using high-resolution printers.

◆ The Cast Vote button has no label indicating its purpose.

The Cast Votes button should have a label "Cast Vote" to clearly indicate what voters should press to cast their vote.

Zerflow recommend placing a Cast Vote Label on or around this button.

♦   More handles are required on the voting machine.

More handles are required on the case of the voting machine to ensure safe carriage and minimise the risk of personal injury.

7 Conclusions

Zerflow have concluded that the voting machine is currently unsecured. The voting machine needs to have the front panel secured to prevent interference with the ballot card. The keys used to access the control console can easily be copied and even ordered by using the serial number on the key. Zerflow recommend the use of 2-factor authentication to secure access to the control console. This would require considerable development time and might not be possible to implement before the election.

The control console keys should never be stored with their respective voting machines. The keys should be delivered separate to the polling station in sealed packages to the presiding officer. The presiding officer can then issue the keys to the relevant staff and prepare the voting machines for the election.

If these and the other high level recommendations made in the technical summary were implemented, the physical security of the voting machine would be greatly enhanced. Strict procedures and policies will also be required to ensure the overall integrity of the election. Such policies would include the management of voting cartridges before, during and after the election.

Separate policies would also be required in the event of a voting machine being damaged and needing repairs. The cartridges should never leave the polling station unless secured by Gardai or other trusted parties.

Zerflow recommend creating formal policies and procedures to cover all eventualities regarding the voting machines and their use. This may not be possible before a May 2002 election, but it is strongly recommended before the system comes into full use.

It is also recommended that a third party audit be put in place to test the system on polling day in the next election, and to measure its performance.

A final recommendation would be to carry out a post election audit following the initial trial in the three constituencies in May 2002.

APPENDICES

Appendix A - Document Control

Version History

Version	Date	Comments
1.01	19/03/2002	Release Draft by Tony Geraghty
1.02	22/03/2002	Draft by Colin English
1.03	27/03/2002	Release Draft by Colin English

Document Distribution

Name	Location	Responsibility	Action/ Information
Tony Geraghty	Dublin	Sales	Info
Colin English	Dublin	Consultant	Action

Document Reviewed By

Name	Location	Responsibility
Tony Geraghty	Dublin	Consultant

Source File Location

..\Customers\Dept_of_Environment\Electronic Voting\deptenviroment103.doc

Appendix B – CE Certification

What is CE?

CE is mandatory for a wide range of products that will be sold or imported into the European Union (EU). The CE Marking regime requires companies to ensure that their products comply with the mandatory health and safety requirements spelled out in EU directives. Without a CE Mark, exporters could lose access to the EU market. Products that do not meet CE may be held at EU member state borders for failure to have the CE mark. Thus product may be rejected and not allowed into that country.

Scope of CE Certification

A CE certified its product ensures acceptance of use within the EU. Products meet the most inclusive directive, the Electromagnetic Compatibility (EMC) directive. This means that products will continue to function properly in environments that are exposed to electronic emissions. This includes forklifts, radios, cell phones, generators, RF, EMI and ESD, CB's and other electronic equipment.

What CE Means to You

Confidence that your data instrument will function properly in the environment in which you use it.
Assurance that if you are exporting product to the EU, your product will not be rejected because the third-party monitoring equipment you are using is not CE certified.
Satisfaction that your supplier is a company that is dedicated to quality products, services and systems.