q

Questions

Powervote / Nedap Electronic Voting System

proposed for the Local and European Elections in June 2004

J P McCarthy BSc FICS MIEI
Chartered Engineer
Management Consultant

Thursday 18th December 2003

Table of Contents

The purpose of this document is to list some questions which arose in my examination of the proposed Electronic Voting system. The list is quite incomplete.
Extracts may be freely quoted with attribution. I would appreciate a copy of any article quoting from this report. Please send them to info at arkaon.com.

Joe McCarthy 086 245 6788

Q 1. Experts

How many people have seen the code?

In Groenendaal Bureau
In Powervote
In the Department
In Nathean

These are the ONLY people who can comment on the accuracy of the compliance with Part XIX of the 1992 Electoral Act.

Q 2. Nedap Voter Number

As stated in the Nathean Database review, why is the VM voter number retained in the Access database after the mixing of the votes?

Given that this number is retained would this provide the basis for checking the electronic record against a VVAT paper record even AFTER the mixing?

Q 3. Ownership of design and code

The RFT says:

> "8.4 Software
> All software paid for and developed to Department's specification will be the property of the Department."

So the Department owns any code paid for.

What are the details of the draft contract?

Who should own this software?

There can you please supply the source to us for review?

Please explain Mr P Greene's comments to the Joint Committee re the question of licence versus purchase of this code.

Q 4. Returning Officers

What is their responsibility?
Have they the necessary expertise in computer systems?

They purchase the machines from Powervote on the recommendation of the Minister.
Who then owns them?
What team of engineers maintains them?
Where are these engineers based? UK? Holland? Ireland?
What expertise is needed before the election? During the count? Afterwards?

Q 5. MS Access Database

In http://msdn.microsoft.com/library/en-us/dnacc2k/html/acmsdeop.asp
Bill Demas, Microsoft, in a paper dated June 1999 said the following:

> Enterprise applications require scalability, security, and robustness, which can all be implemented with MSDE or SQL Server **but not with Jet**.
>
> For example, if your application needs transaction support, even in the event of a network, server, client computer, or client application crash, you will want to use MSDE or SQL Server.
>
> Conversely, the Jet engine **does not support** atomic transactions: **It does not guarantee** that all changes performed within a transaction boundary are committed or rolled back.
>
> If the system were to go down with Jet, **the database could be corrupt** and you might need to revert back to your last backup copy.

Nobody uses Access for critical databases.
Microsoft themselves recommend the SQL Server code base.

What is the Departments view on the robustness of MS Access?

Q 6. Protection of messages –Etopup, Lotto, Votes

Universal practice in systems used in Ireland is to use cryptographic techniques to protect the integrity of messages.

Systems in everyday use such as the Lotto and the mobile-phone voucher topups in shops use encryption and MACs.

Have you considered these techniques?

Is there a Digital signature on every vote?

What is the dictionary used in your implementation of Hamming codes in the Ballot Module?

What do you do when an error occurs?

Q 7. Hamming code

With 4 copies of each vote recorded in the Ballot Module, what are the rules when one copy mismatches on being read in to the Count PC?

And when two copies mismatch?

Are these rules implemented in the "Dutch" code module?

Q 8. No ERS European tests

Why has ERS not been asked to test the European Election profile?
These are very large counts of up to 450,000 votes.

Q 9. Testing with Multiple Ballots

Pseudo code is in-complete
Has this been completed?

The flowchart is incomplete.
Written by Nathean not by the software developers themselves
Has this been completed?

Have the developers supplied their versions of the pseudo code and flowchart?

Q 10. End-to-end Testing

On Wednesday 17th December 2003, I reviewed 5 large files of correspondence concerning the EMS testing, the ERS testing and the IES testing.

There was NO record of an end-to-end test plan.

One record showed that a small number of votes (less than 20) were entered for a few candidates and moved through the system to a final count.

Q 11. Risk Analysis

Has a formal risk assessment been carried out?
On the VM?
On the EMS?
On the IES?
Can we have a copy of each?

What risks were identified?
What steps have been taken to reduce or eliminate them?

Q 12. Certification

List the certificates issued.

List the accreditation of the certifying agency.

Q 13. Power failures

What precautions have been taken in the VM?
Please provide more details on the debate concerning the interim storage of the vote in the Xicor chip.

What precautions have been taken in the IES PC?

Q 14. Powervote Documentation

There is a no technical documentation for the Powervote Counting system

No manual was sent to ERS for their testing this summer. They had to request one. It is not clear if one was supplied.

Who wrote the system specification?

Where is it?

Reference in PMI report to a Technical Documentation CD – page 8 of the Database Evaluation report dated 14 December 2001.

What is this CD?

Why did the Department not reference it in any of their replies to my FoI requests?

Q 15. Nedap Documentation

There is a body of documentation for the Nedap Voting Machine

See list on pages 8 and 9 of ESI1_Software document.

Released records x

Refused records y

Why not release the documents withheld?

Particularly the document entitled:

Reliability of the Voting System ESI1, RBW Teunissen, Ver 1.1 dated October 2001.

Q 16. External Reviews

Has your system been reviewed by a large number of outside security experts?

If so, who?

What are their credentials?

Do their areas of expertise cover a wide area of specialities?

- within the discipline of cryptography
- computer security
- formal code development methods

Can we see an executive summary of their reports?

Can we have the full reports?

Q 17. Source Code

Do you allow the public to review the security and reliability of your voting system's source code?

If not, why not?

Is the security of your system dependent on your source code being secret?

If so, how do you address the fact that the source code could leak to the public (or to well-funded adversaries)?

And how do you address the fact that an attacker might be an insider who knows the source code?

Q 18. Outside Security Expert Review

Would you be willing to have a panel of outside security experts review the source code for your system?

Would you allow them to publish an executive summary of their findings?

If not, why not?

Q 19. Designer

Who designed and developed the source code used in your systems?

What are their credentials with respect to cryptography and computer security?

Where were they trained?

Have these developers worked on cryptography and computer security in other systems outside of voting software?

Q 20. Vendor

How confident are you in the security and reliability of your product?

Will you "certify" the security and reliability of your product?

Will you offer a full refund, plus "damages," if we purchase your equipment and later find that it is vulnerable to certain types of attacks? (Which types of attacks?)

Will you offer a full refund, plus "damages," if after an election it is determined that more votes were collected than people who voted (on a given machine), but that it cannot be determined which were the legitimate votes?

Will you offer a full refund, plus "damages," if after an election it is determined that your machines reported an inaccurate total (either because of an attack or a system glitch)?

Will you offer a full refund, plus "damages," if after an election it is determined that voters' anonymity was compromised, allowing votes to be bought and / or sold?

Under what other situations would you offer a full refund, plus "damages?"

Q 21. Assurance to the Public

In your system, what can voters do if they feel that their votes were not recorded properly?

Are there any mechanisms for voters to verify their votes are correct?

What happens in the case of a dispute?

Is a manual recount (i.e., not requiring any computer software) possible?

Q 22. Cosmic Rays

Any system with a large number of machines will experience soft errors due to Cosmic Rays. These high-energy particles occur naturally all the time and will strike the electronics of computer systems in an unpredictable manner.

These particles cause soft errors in memory. The results are unpredictable but their frequency is well understood.

These incidents are called Single Event Upsets (SEU) in the literature.

We have direct evidence of one incident in Belgium and two in Ireland.

Cisco research paper

"Increasing Network Availability" a white paper by P Martson dated 26 May 2000 is available at
http://www.cisco.com/warp/public/779/largeent/learn/technologies/ina/IncreasingNetworkAvailability-FAQ.pdf

The following is an extract from this paper:

The use of ECC will decrease the soft FIT rate to a value at least as small as the hard FIT rates (this is influenced by system design and how data bytes are mapped to memory components) which, as described earlier, is one or two orders of magnitude smaller. The FIT values for hard failures are often in the range of 5 to 20, as detailed in Table 2 below.

Table 2: Projected SRAM hard and soft error rates, equating ECC with FIT rates at least as small as hard error rates

	5 FIT	**20 FIT**	**100 FIT**	**200 FIT**
Number of VIP2-50s	**Average Time Between Hard Errors**		**Average Time Between Soft Errors**	
	With ECC		***Without ECC***	
10	71.35 years	17.84 years	3.57 years	1.78 years
20	35.67 years	8.92 years	1.78 years	10.7 months
50	14.27 years	3.57 years	8.56 months	4.28 months
100	7.13 years	1.78 years	4.28 months	2.14 months
200	3.57 years	10.70 months	2.14 months	1.07 months
500	1.43 years	4.28 months	3.72 weeks	1.86 weeks
1,000	8.56 months	2.14 months	1.86 weeks	6.51 days
2,000	4.28 months	1.07 months	6.51 days	3.26 days
3,000	2.85 months	21.70 days	4.34 days	2.17 days
5,000	1.71 months	13.02 days	2.60 days	1.30 days

Note the value highlighted at the bottom right. This predicts an SEU every 1.3 days in a population of 5,000 machines.

The VIP2-50 supports 4 to 8 MB of SRAM and 32 to 64 MB of DRAM not unlike the amount of memory used in the IES systems.

Since we have some 6000 to 7000 machines in the IES system in use can we expect an error every day?

What precautions have been taken by the designers?

In the VMs?

In the Count PCs?

The Schaerbeek Incident.

Le collège a été prévenu d'un incident à Schaerbeek le 18 mai à 23h30.
4096 more votes counted than cast.

At a polling station in Schaerbeek in Belgium on 18th May 2003, a candidate received more votes than his party list.

See http://wiki.ael.be/index.php/ElectronicVotingRandomSpontaneousBitInversion for details.

The Belgian e-voting expert David Glaude reports an incident with e-voting in Belgium. Not widely published it took place on 18 May 2003, in the municipality of Schaerbeek. The total number of preferential votes cast for a specific candidate was higher than the total number of votes for his list.

A series of tests was conducted on the computer of the president of the voting committee, but the error could not be reproduced. The difference in votes was exactly 4.096, leading the research-team to the conclusion that the error was probably due to a spontaneous inversion of a binary position in the read-write memory of the PC.

The Belgian e-voting system is fairly complex, with a blank magnetic card that every voter has to insert into a voting machine. After voting, the card must be entered into a ballot-box. Attached to the ballot-box is a computer with a floppy-drive. The voting-results are written on a floppy-disk.

See the official report (in French) from the Collège d'Experts at http://www.poureva.be/article.php3?id_article=32

An investigation began on May 19 in the presence of the president from canton, representatives of the SPF Intérieur, companies Steria and Bureau Van Dijk and college of experts.

5.3.7.3 Conclusions of the college on the incident of Schaerbeek:

Since no error was found in the software, and considering the internal structure of the program, the college concludes that the error was most probably caused

by a spontaneous and random inversion of a binary position (this phenomenon is abundantly described in the specialized literature).

BM 367 Limekiln

A failure occurred with Ballot Module, number 367 of Dublin South West – used at St Paul's Senior and Junior Primary Schools, Limekiln.

It had a "*blocked - checksum not in order*" failure and was sent "*to Nedap for a report*".

This failure shows that computer systems do fail sometimes. This is one part of the Irish Electronic Voting system that has failed.

It may have failed due to a "Single Event Upset".

Error 7002 Xicor chip write and failed readback.

On 14 Dec 2002 Powervote reported an eplanation for an error 7002 in Voting Machine P3D000578 used in Dubln West for the Dail 2002 election. Staff at the polling station reported that the machine had this error.

The explanation was *"...the Xicor chip wrote a code and it detected that the read back was not correct"*.

This almost certainly was caused by an SEU. Powervote offered no further explanation.

See also http://www.pcguide.com/ref/ram/err.htm for details of memory protection schemes including parity, false parity and ECC.

Note that the recommended PC for the Returning Officers does NOT support ECC.

Conclusion: The Irish voting system will suffer one of these events in every election.

What does the Department propose to do about this?

Q 23. Multi-user or not

Statements to committee that PCs will be standalone.

There detailed provisions in the system and in the instructions and in the testing for multi-user implementation.

Which is it?

What is the performance of a single machine counting up to 450,000 votes in a European Parliament constituency?

Q 24. Performance

How fast are these machines at reading in the ballot modules?

For General elections?
For European Elections?

How fast are these machines at counting?

Please detail the logistics for the European elections?

Q 25. Maintenance free statement

Machines have already been sent back to manufacturers to have a chip replaced.
Which machines?
How many?
Why?

PCs do not last 20 years.

Has an assessment of the engineering maintenance been done
What are the results?

Q 26. Petition Logic

This complex aspect of the software had not been developed or tested in the records I had sight of.

What is the current state of development and testing?

Is it still proposed to re-adjust each ballot to remove preferences for dis-qualified candidates?

If so, does this procedure interfere with the ballot as cast by the voter?

Is this constitutional?

Q 27. Vandalism

Superglue, magnetic fields, chewing gum, brute force, a penknife?

What risks have been assessed?
What precautions have been taken?

Q 28. Sabotage

Manufacture and programming is done outside the jurisdiction of the Irish Courts.

What risk does this pose to the Irish voting system?

Q 29. Capacities – 5 elections - 56 candidates – 18 LEDs

What are the limits on the VM and in the IES?

For local elections candidates need 15 registered voters for nomination.

If, say, 1500 people nominate 100 candidates, what happens to this system?

The constitution permits this.

Originally 28 Buttons / LEDs per column – now it is 18.

So does the max of 56 candidates per election now become 36?

Q 30. Secure Coding Methods

Were any used in developing these systems?

Which ones?

Was Bruce Schneier consulted?
Was Ross Anderson consulted?

If not, why not?

Q 31. Security

What security is used to protect each vote in the Access database?

Security by obfuscation is no security.

Example is the A5 algorithm used in the GSM standard. The manufacturers did not allow open review – it has now been cracked.

Q 32. Development model

The Nathean Code Review Guidelines, dated 14 December 2001, on page 3 says:

> "Typical code reviews should address the following questions:
> 1. Does the code implement the design as specified in the design document?
> 2. Does the code have unspecified side effects?
> 3. Does the code follow your style guide
>
> As PMI Software is not the developer of the system, we cannot establish if Powervote's style guide has been followed so we have concentrated on 1 and 2"

Nathean therefore could not carry out task 3.

Does this mean that nobody has checked the style guide used by Powervote?
Can we have a copy of this style guide?

Q 33. Haste

Why is there a rush to implement?

Paper voting for over a century has resulted in a stable situation with:

- Detailed Statutes
- Established case law
- Vast experience
- Public ownership of the process

Can you define the net benefits to the public for this investment?
Can you cost them?

Q 34. Cost

The Department has not done a cost analysis.

Every VM needs a control operator – this is one more person at each polling station.

What are the explicit costs for the IES software part of the contract?

The voting machines cost € 5,008 each plus VAT with a 10% discount for 6000 machines.

Q 35. Indemnity

Will Powervote indemnify the Irish people that this system will faithfully implement Part XIX of the Electoral Act 1992 as amended?

Q 36. Quality

Who is responsible for the quality of the whole system?

It seems that this task has fallen to the Department. They do not have the necessary expertise and must rely on external companies. They have chosen just two: Nathean and ERS.

What tendering process was used to select these two companies?

Q 37. C&AG

Has the C & AG done a value for money audit?
What is the result?
Can we have the report?

Q 38. Suppliers

Please explain the relationships between

- Powervote Ireland
- Powervote Services Ireland
- Powervote UK
- Nedap
- Groenendaal Bureau

Who owns shares in these companies?

Who gets the profits?

Q 39. Spot Checks

Can we select random VMs for a paper check?
Can we select a random constituency for a n audit?
Who should conduct these audits?
Do we need an electoral commission to do this?

Q 40. Legato – Hot backup

Financial systems used in Dublin use techniques based on Legato Software to ensure a second copy of each record is safely written before the software continues.

Have such techniques been considered here?
For the Voting Machine?
For the counting machine?

Have write only media such as CD-R been considered?

Q 41. Dutch Code

The Nathean report pointed out certain modules with dutch comments and function / variables names.

Has a version written in English been supplied?