

e-voting Security Study Response

by Jason Kitcat
The FREE e-democracy Project

Background

In this response my aim is to present opinions and findings formulated after three years spent studying and developing Internet Voting systems. Our Internet Voting system, GNU.FREE, is a part of the Free Software Foundation's (FSF) GNU project and is the only voting system available under the GNU General Public License. I have also worked on behalf of the FSF to represent Free Software views on the committee of the OASIS election services XML standard. My award-winning thesis for a Bsc(Hons) [Computer & Business Studies, Warwick] explored how the Information Revolution is changing the political process.

I have worked with communications technologies for the past 8-9 years; first running a modem-based Bulletin Board System before moving onto the Internet and creating several award-winning sites. Currently I am co-founder, Head of Production and a director of Swing Digital Ltd. a small, Brighton-based, Internet consultancy specialising in online communities especially for alumni. I designed and built Alumni[net], our integrated web community product.

1. Should the proposed "key principle" (para 59) be adopted?

Yes. But it perhaps needs to be communicated with more clarity.

2. Is the security profile set out in Annex A of the report valid and complete?

It is an excellent start. I would be loathe to say that any security profile can ever be complete... just always approaching completeness. One additional threat I would suggest is that of cryptographic attack. If a cracker understands the system used to generate PINs, response codes or whatever other crypto-based token the voting system is using it may be possible to create new, valid codes which have not been issued to other voters. (In the same way that valid, but non-existent, credit card numbers can be easily generated.)

3. Should Annex A be adopted by Government as the foundation for securing the 2003 pilots?

Yes. However I would advocate very strict assurance procedures (not a short-cut process such as FASTTRACK). One must recognise that every time the smallest modification to software or hardware is made, all previous security assessments are rendered invalid as any number of new security problems can be introduced. An independent lab with sufficient resources and experienced resources should be created if HMG wants to see widespread electronic voting.

4. Is CESG right to conclude (para 69) that current security technologies are not able to meet all the requirements implied by the key principle, the security profile, and recommendations 1-5? If so, what strategy should be adopted?

Absolutely correct. Current security technologies cannot create an adequately secure and private remote Internet voting system which has the reliability and scalability to deliver national elections. Most security systems are brittle (they either are secure or they aren't, no fail-safes, no second lines of defence) and all computer software has security vulnerabilities.

A long term strategy of small pilots and funding research into computer security should be commenced. Electronic voting in polling stations is viable in the medium term, but I would recommend extreme caution with regards to REV.

5. Is a scheme broadly in line with Annex C:

a) theoretically sound?

There is little detail, but of what I can see it is workable and thus theoretically sound.

b) likely to be implementable by suppliers?

Yes. However this system already exists and has been patented by Dr. David Chaum who has setup a company to deliver voting solutions, SureVote (<http://www.sure-vote.com>). I'm not sure how happy they would be to have others use it, though David has mentioned to me a potential desire to Open Source some of their voting software.

c) likely to be manageable by electoral administrators?

There are clearly issues with the security of generating and reliably distributing the necessary codes to voters. These may prove very costly to solve.

d) likely to be usable by, and acceptable to, voters?

From a computer science perspective there is a simplicity and beauty to the system, however sets of numbers and computers are likely to be discouraging to some voters and will seem complicated in comparison to pencil and paper. A reliable way to allow disabled voters to use such a system would also need to be developed - what are the costs of brail cards with codes?

e) achievable in a pilot in May 2003?

It will be a tight run thing unless SureVote take part with their software which matches this scheme. Election companies may say that it is doable but none of the others use this system. To modify their existing infrastructure or build new systems from scratch; plan all the management issues and polling stations infrastructure and also gain assurance on the security of the system

in what will be a short time once the bidding process has been completed will be tricky. Corners will be cut – how will the government be able to verify the security of commercial provisions when in a hurry?

6. Are the other recommendations sound? Is anything missing?

Firstly, I want to say the quality of this report is excellent. Most of the existing prior art and best practice is well represented (though I was surprised to see the omission of work by David Chaum and also Josh Benaloh-Cohen) and thank you for the mention of GNU.FREE. I support all the recommendations in this report.

Now, a couple of issues:

- **Turnout**

This report has a worrying pre-occupation with associating the move towards electronic voting as a policy to re-engage the public in the political process and improve turnout. Even the Government's e-democracy consultation paper *In the Service of Democracy* makes it clear that turnout is unlikely to be effected by new voting channels. All the evidence supports this view as I have detailed in my response to the e-democracy consultation and at <http://www.free-project.org/writings/trt.html>
- **Counting**

One area that has not been explored in this report is the issue of electronic counting and recounts. If an administrator recounts with the same counting machine then she, at best, merely verifies the reliability of the counting machine – NOT it's accuracy. It may be making the same errors (accidental or malicious) consistently on each count. The only trusted way of recounting is to use a completely different counting system from a different source. Furthermore there are many convincing arguments for creating a paper-based backup of votes for such eventualities.
- **Clients**

I have to disagree with the report's view that intelligent client software is less secure than using a 'dumb' interface such as the browser. If we assume that both run on equally insecure operating systems then both are at risk. But all popular browsers have plug-in architectures which allow third-party software to be installed into the browser with no security or trust architectures in place. Because modern browsers try to deliver so much functionality (email, HTML editing, multimedia, XML, HTML display etc) they consist of huge amounts of code, all of which can contain vulnerabilities. The quality of the code cannot be determined by the breadth of use nor by the company who built the browser in question. The most popular browser, Microsoft Internet Explorer for Windows, also has the most security problems as a very serious recent vulnerability in IE's

SSL implementation illustrates. (See <http://online.securityfocus.com/archive/1/286290/2002-08-08/2002-08-14/2d> for more). Within this context I would argue that a single-use item of software (such as a Java client) delivered in a secure manner – preferably offline with a CD-ROM, is significantly easier to audit and verify as secure than the indeterminate number of variations possible in the browser world.

- **Academic Survey**

The attitude within the survey of academic work indicates that the authors of the report regard the academic opinion as quite conservative and not sufficiently pro-electronic voting. For example in para 124:

Professor Rivest holds a more balanced view on electronic voting than his peers

The academics reviewed have spent considerable amounts of time studying computer security issues and voting in particular – it is perhaps wiser to think about why the majority are opposed to REV rather than writing them off as being unbalanced.

I would like to highlight section **B.8.4** and amplify the difficulty in creating a secure, private and reliable Remote Internet Voting system.

I would also like to draw attention section **B.8.6**; this is an important point which is the subject of much debate in academic and commercial circles as well as in the OASIS committee. This is especially a problem if the audit trail is only computerised. Bruce Schneier's idea of providing a paper-based audit trail is probably the best way of resolving this issue... though any computerised voting will need some level of computerised logging. In our system, GNU.FREE, we offer two levels of detail and allow the voting administrator to determine how much to store with the knowledge that more detailed logs could be abused to undermine voter privacy.

Finally I would like to draw attention to section **B.8.10**, this is a fundamental issue which goes to the heart of ensuring the public trust the system. But furthermore it goes to Kerckhoffs's principle: In good crypto systems, Kerckhoffs wrote, "the system should not depend on secrecy, and it should be able to fall into the enemy's hands without disadvantage." Thus keeping the workings of a system secret is a bad sign for its overall security. Yes, the systems should be fully audited and assessed by the government. But it is my opinion that unless independent third-parties (NGOs) have access to the full systems, including the source code, then it will prove difficult for the public to put their trust in any proposed electronic voting system. Such third party scrutiny should be a core part of any plans

to computerise our votes.

- **The Dangers of REV**

I fully support the notions set forth in section **B.8.14**, the current assumptions by many politicians with regards to REV, and the subsequent timetables laid out need to be questioned. REV is extremely complex and difficult to deliver – I know because I've built such a system. Managing the security risk with current technology and academic thought just isn't possible. As quoted by the report, from his excellent Crypto-Gram emails, Bruce Schneier has wonderfully stated:

[an Internet Voting System] would be the first secure networked application ever created in the history of computers.

The FREE e-democracy Project

<http://www.free-project.org>