

Furthur down the road... Why voting shouldn't be electronic.

By Jason Kitcat, j-dom.org (originally published in LinuxUser)

Those who may have caught my previous LinuxUser article about the FREE e-democracy project will know that I have a long history with electronic voting, both building and researching systems. However I no longer believe that we should aim to build electronic voting systems for our elections and I'm here to explain why this is the case. Essentially I'm here to challenge the concept of technology being 'progress' no matter what the specific details of the case. The 'technology is progress' view brings to mind Ken Kesey and his Merry Pranksters who named their bus and modus operandi 'Furthur'. While I'm in favour of 'progress' in some cases I get the distinct sense that electronic voting is a bus with eager politicians and technologists bouncing along in the driver's seat going furthur whether or not we want it to.

Who are you?

One of the most important processes in a fair and free election is the verification that a voter is entitled to vote and hasn't already cast a vote. At first blush this seems like quite a simple problem, even to experts, but in fact it's an extremely complex one and the debate over ID cards rehearses many of the same arguments.

If one examines the current UK process for authentication in a polling station all one needs is the polling card sent to your address. You may be asked for some other identification but it is unlikely. You are then crossed off a list of voters and allowed to vote in a booth using a numbered ballot. The number on the ballot ties to the list you were ticked off thereby allowing your vote to be retrieved and examined in any investigation that may arise. (See box) This is a rather weak authentication process, especially considering the polling cards are sent unsealed to your address allowing easy interception in the postal service. There have been several reports of dead people voting and also nurses voting for all the patients in their care without consent.

In an electronic scenario this mildly worrying situation descends into downright disturbing. Currently there are no practical electronic methods for certifying that a user really is who they claim to be. Certificates and smart cards can authenticate a computer but not the person using it – the token (the generic term for security tools such as certificates and passwords) may have been taken by someone with malicious intent or the legitimate owner may have logged in and then left their computer unattended allowing a third party to impersonate them in a vote (or online bank etc). Biometrics are not a solution either, fingerprint scanners can be easily tricked with gelatine imprints and other scanners are prohibitively expensive. Furthermore if the database of biometric tokens is compromised in any way we have a huge problem – we can't issue new retinas whereas as least PIN codes can be changed if we know someone might have seen our current one.

But even if we could be identified accurately online an electronic scenario provides other problems: Our traceable votes would be so easy to rationalise into a table showing how each citizen cast their vote that abuse would be significantly more likely. When discussing abuse one must not imagine just the hypothetical lone

cracker but also more serious attacks where parties or collections of candidates work together for a mutually beneficial outcome. This could be altering the result of the vote or retrieving data on which citizens need more 'work' before they vote for the 'right' party next time.

Some politicians have argued that the threat of a jail sentence in the electoral legislation is a sufficient deterrent to potential fraudsters, however the realistic chances of being caught are extremely slim. Of particular concern are postal ballots where fraud is virtually impossible to detect with the current legislation and processes. Electronic votes might be worse, particularly if one considers how much the complexity of technology can obscure what is really occurring in a system. The cost of implementing even a flawed authentication system which might include issuing smartcards to all citizens would be prohibitively expensive if one factors in not only the cost of the cards but the need for universally available card readers. This also ignores the increasing ease with which smart cards can themselves be compromised and copied which would inevitably force the authorities into an expensive technological 'arms war' with ID card crackers.

Did that work ok?

If we magic away the huge authentication problems then the fundamental problem for electronic voting to solve is how to allow each voter to anonymously but reliably record their preference only once. This is an extremely tricky problem completely unlike ecommerce. Thus when security experts hear a politician (or salesman) claim that "If we can bank online why can't we vote online" they grit their teeth and begin planning ways to climb up the walls.

Ecommerce works because we are not anonymous. Firms effectively hedge their risk by sucking as much identifying information out of us as possible, thus if anything goes wrong they can track us down and try to get their money. This is why, in many respects, the Internet is a huge boon to the police fighting illegal activities because credit cards leave a huge data trail across the net which fingers not only the users but the sellers too. Pete Townshend can testify to the effectiveness of this new capitalist crime-fighting tool.

Unfortunately we can't have such incredible traceability if we want people to trust an election. There are cryptographic ways of trying to separate the voter from their vote which work to a greater or lesser extent, the best solutions are virtually impossible to implement in the real world. Thus in a real world solution we can get a reasonable approximation to an anonymous vote... but an administrator with sufficient access and time could well pull together the logs to various parts of the system and figure out within a reasonable probability who voted what. Some commercial systems actually send the vote and user data in one packet which would make the job significantly simpler, our enterprising hacker would just need to sniff the data after the SSL stream was decrypted. The paradox is that while we want to strive for an anonymous vote we also need auditability to try and catch any attacks, the more we improve one, the more the other suffers.

Of course there are so many ways a complex computer system can be compromised it's almost not worth exploring, but from my conversations with people on the topic too many are completely unaware of how vulnerable systems could be so here's a rundown of my top concerns for any e-voting system.

- **Client System Compromise**

A trojan, virus or operating system hole could allow an attacker to view how a user has voted, manipulate the outgoing vote or prevent it from being sent at all but give the user the appearance of a successful vote (quite a nice attack, I think, with the right data you could prevent just the right number of a certain type of voters from succeeding and 'encourage' a win for your party and yet the data would look perfectly valid).

- **Client Software Compromise**

Many proposed systems rely on the web browser as their client interface. This is a terrible idea when one considers the number of plug-ins and features lurking in the code of the average browser, none of which are checked and could hide any number of malicious trojans. Custom-made client software is likely to be more secure but distribution is a huge problem – a cunning attack could involve issuing fake client voting software.

- **Denial of Service (DoS) Attack**

While this would be unlikely to swing the outcome of the vote it would be relatively easy to prevent the election from occurring. With the current setup of the electoral roll in the UK someone who had registered to vote online from home (or mobile phone) would be unable to vote in a polling station in the event of a DoS attack. One can certainly imagine not only protest groups but even hostile nations being interested in using this simple but effective attack which has no effective defence.

- **Reliability of Infrastructure**

There a huge number of sub-systems involved in a successful electronic vote. Even if they work reliably with no problems there are opportunities for staff in many organisations to disrupt or fully stop an election by attacking the communications infrastructure in telephone exchanges, service providers and hosting centres. Electricity is also a mission-critical resource across the nation in an electronic vote.

- **Incompetence**

Setting electronic voting systems is likely to be a complex task which few understand and an even smaller number will get totally right. The smallest error can compromise the security and anonymity of a vote.

- **Trusting the Administrators**

There are a large number of volunteers and paid staff in any election. They are trusted parts of the system, but we do have some checks in place such as allowing candidates to watch the count to keep the admin staff honest. The opaque nature of electronic systems makes it significantly more difficult for us to watch the admin staff. Thus the trust we put in them increases and the

potential damage they can cause also grows.

- **Closed Source**

All the systems currently being evaluated or used by the US and UK governments are closed source, no third party has been allowed to assess the design and implementation of the systems. Thus not only could malicious backdoors be present to undermine an election result but innocent errors could also be lurking to cause problems. Ideally the source should be available for any citizen to examine but this still presents huge problems... How do we know that the published source is actually that used in the live system? Every time there is bug-fix or update do we re-audit all the code? We should. One fix can introduce three more bugs or could hide a cunning exploit for future use by a disgruntled employee. How do we check that each server or kiosk is indeed using the code that has been audited?

Crossing the Great Divide

There's a more subtle issue which might impact the results of an election but isn't being effectively addressed. The digital divide is an issue which has been bubbling along in the new media sector for quite some time and there can be no doubt that it is a genuine phenomenon. Computers, and the Internet in particular, are a playground for educated, middle-class young males.

While I have strongly argued that electronic voting is unlikely to increase voter turnout, if a large number of issues are polled in a primarily electronic manner then this will create a distortion in the results due to the demographic makeup of the online world. Polling organisations have recognised this and a recent ICM report highlighted the huge errors polling online generated.

There is a deeper issue at hand too, are we willing to send the message to those disadvantaged citizens who are not online that the government is willing to spend significant sums of money making it easier for a primarily well-off constituency to vote? Is it so tough to vote now that the development of electronic voting is desperately needed? Couldn't the money be better spent on the people who need it most? I shall return to the cost issue later in the article but it's clear that nobody has yet provided a satisfactory answer to these questions.

Trust me, I'm an expert

In the pilots we've seen so far the suppliers and administrators have been asking voters and candidates to trust the systems and their results because they've been built and run by 'experts'. We haven't been able to assess the level of fraud, the detailed working of the systems used or have a second, parallel, voting channel to assess how accurate the electronic results really were.

If we accept only some of the problems I've raised then I have great difficulty believing that voters or candidates and their parties will be willing to accept the results of electronic votes. The chances of the results actually being a fair and

accurate reflection of the people's intentions seems quite slim. Certainly asking for a recount won't help, due to the peculiar nature of computers a recount is meaningless.

This is an important point so let me explain by introducing an imaginary function which is useful for some purpose. If this function is $1 + x = y$ where x is the input and y is the useful number then we have a very simple sum. Imagine that x is 6, every time we run the function we will always get $y = 7$. Simple enough, and this is how electronic vote counters work (if they are counting electronic votes and not paper ones). Each time you recount you will get exactly the same answer from the database. What this doesn't tell us is if it's the right answer!

With paper ballots we can look at the piles of ballots to make sure the number we get is the right order of magnitude, then we can look at each ballot to make sure they are in the right pile and if still unsatisfied we can get a different person or machine to count the paper ballots. Getting someone or something new to count the ballots is like introducing a new function which still gives us y but by a different method. So if we have a new function $(x - 1) + 2 = y$, plugging in 6 still gives us 7 so we can apply it to all our data and make sure we are getting the right answers for y from the original function. Obviously these functions are useless and very simple but we can't even do that with the electronic votes sitting in a database – they are just numbers with only one function to count them. If we had a paper printout of the vote a citizen entered into the system then we could count all these up and check the number against the electronic result, we'd have two separate functions to verify our y value.

Thus a good way to ensure the results are accurate and will be respected by the candidates is to have paper ballots (or some other reliable second channel). Clearly we can't easily do this with remote e-voting so we are faced with the prospect of kiosks in polling stations with paper printouts. So for the benefits of quicker preliminary results and potential greater ease of use (though existing systems are reportedly not easy to use at all) we will need to spend huge sums of money on systems which still need paper to keep them honest. Is it worth it? Couldn't we spend the money on something better? I think so.

Conclusions

I argue that for any major electronic election to be successful and its result adhered to by the candidates any system used would have to be:

- Secure
- Private
- Open
- Reliable
- Scalable

When I originally formulated those criteria I felt that Free Software would allow us to achieve those fundamental goals. Now, after trying to build such a system and watched others try too I'm of the opinion that it cannot be done with today's

technology. However if we are forced down the road of e-voting by politicians there can be no doubt that it should be done using Free Software.

Let us focus our energies to turning our Free Software bus, GNUFurthur, to e-government. Voting works rather well as it is, but Free Software has huge potential benefits in electronic government applications that we need to communicate to our governments. Only with Free Software can our tax money go further.

BOX OUT

Free and Fair Vote?

Most democratic countries put a huge emphasis on the anonymity of the vote. But here in the UK each vote can be traced back to the voter – in theory this can only be done with a court order but we have no way of knowing how often this has been abused. When working on an international standards committee for electronic voting my non-British colleagues were shocked when they heard this. They had been arguing for the standard to champion best practice by forcing anonymous votes in all implementing systems. An embarrassed debate ensued when it became clear that 'best practice' would exclude the UK and wouldn't be possible considering our Office of the e-Envoy was sponsoring the standard!

In fact a report on implementing e-voting written by de Montfort University for the Office of the Deputy Prime Minister has pointed out that traceable votes may be in breach of several British treaty commitments including:

- Universal Declaration on Human Rights - Article 21 (3)
- International Covenant on Civil and Political Rights - Article 25
- European Convention on Human Rights - Protocol 1, Article 3
- OSCE Copenhagen Document of 1990
- Inter-Parliamentary Union Declaration on Criteria for Free and Fair Elections (Paris 154th Session, March 1994) - section 2(5), 2(7) and 4(5).

As a result there may be wider reforms to remove this requirement from all elections and not just electronic votes.

BOX OUT

Swimming against the tide

There's a long and distinguished history of writers, both of fiction and non-fiction, eloquently expressing their doubts over the onward march of technology.

Many regard the beginning of modern 'anti-technologism' to be the English workers' protests in the early 1800s led by 'King Ludd' who lent his name to luddism and luddites. Generally being called a luddite has somewhat derogatory implications, the wearer of such a badge is portrayed as being against technology no matter what the benefits. However, according to historian E.P.Thompson, King Ludd had a rather

subtle view on technology including opposition to what we would now call the free market. He'd probably fit right in with today's anti-globalisation movement.

Since King Ludd we have had many critiques following in the Luddite tradition including George Orwell's media, technology and political critique '1984' as well as Aldous Huxley's dystopia 'Brave New World' which if read with his utopia 'Island' provides an extremely thorough provoking appraisal of science and technology.

Relevant non-fiction authors include Neil Postman who has written superbly critical books such as 'Amusing Ourselves to Death' on television and 'Technopoly: The Surrender of Culture to Technology'. A wonderfully readable critique directly aimed at computers and the Internet is 'Silicon Snake Oil' by Clifford Stoll (an astronomer and renowned geek) and reads well with Howard Rheingold's 'The Virtual Community' which at first blush seems positive about the online world but manages to ask some vital questions while telling the story of how the virtual world began.

Related Links:

Superb links & resource page for Luddism and related topics
http://carbon.cudenver.edu/~mryder/itc_data/luddite.html

Luddites entry from Wikipedia
www.wikipedia.org/wiki/Luddite

LINKS BOX

The FREE e-democracy Project
www.free-project.org

Office of the Deputy Prime Minister Election Section
www.local-regions.odpm.gov.uk/elections/index.htm

ICM Report on Internet Polling
www.icmresearch.co.uk/reviews/2002/Internet-polling-paper-jan-03.htm

Ken Kesey and the Merry Pranksters
<http://www.key-z.com/>