Electronic Voting

With the elections looming in America, the issue of the security of electronic voting is back in the news. Both major parties are making serious allegations that the election may well be rigged. Its outcome may even be determined by interference from a foreign government. This extraordinary movie-plot possibility is made plausible by the widespread use of Electronic Voting machines – which are based on computers which may be vulnerable to undetectable hacking.

Back in 2002 we in Ireland had our first experience of electronic voting. And I can claim the right to comment on the issue as I wrote part of the subsequent report that resulted in the proposed scheme being scrapped. I can in all seriousness claim to have helped to save Irish democracy.

The report was rather an embarrassment to the government of the day, so its not surprising that it can no longer be found on government websites. But the internet never forgets..

http://www.umic.pt/images/stories/publicacoes1/Appendix%202B.pdf

Basically the government decided that to make the counting of votes simpler, electronic voting machines could be used, as after all one thing we know computers can do well, is that they can count. And all there is to electronic voting is the ability to count votes – right? So 50 million Euro was spent on a Dutch machine. One of these simple machines would reside in each polling station, and voters would click on their candidate of choice, the votes for each candidate would be tallied, and at the end of the day the votes would be extracted onto a storage medium and transferred securely to the counting centre, where all of the votes from all of the polling stations would be totted up on a central computer, and the winner determined. What could be simpler.

The idea seemed to be the bees-knees in modernisation. We were going to lead the world! Some luddites muttered but our prime minister famously hit them with the put-down line “Give up your Aul pencils!”. A pilot scheme was organised for the 2002 election in some constituencies, and it all worked quite smoothly and at devastating speed. One government minister who lost their seat, was so visibly shocked and upset that they had to be led out of the room, and later described the experience as being like “a sudden death”. The media lamented that the sheer speed of the process removed all of the drama and tension, the kind of thing the media love. That appeared to be their only concern.

Anyway our report was commissioned, and the Dutch system scrapped. The tax-payer lost a heap of money, reputations were savaged, as a nation we all rather felt we had made fools of ourselves. But at least we learned our lesson. We won't be using electronic voting again any time soon. (Unfortunately the manufacturers of Electronic Voting machines still succeed - especially in America- in getting gullible state officials to buy their products, dazzling them with techno-babble.)

So now in 2016 we are back to our “aul pencils”. But how did it all go so horribly wrong? Well the basic problem was that the proposed method was completely insecure.

To understand why, first you need to clear your head of the notion that manual methods of doing things are intrinsically naive and stupid, and that technology based solutions will always be superior. It turns out that our manual voting system may be slow but it is highly robust against external threats to its integrity. Electronic Voting struggles to achieve the same level of robustness, and indeed even now despite years of research, its still not good enough to replace the manual method.

Which is not what the people want and expect! There would certainly be huge advantages if secure Internet Voting (which is where we had assumed electronic voting was heading) were a possibility. But, perhaps surprisingly, its not, not yet anyway.

The issue that lies at the heart of this problem can be summed up in one word. Trust.

Who do you trust? Do you trust the machine manufacturer? Do you trust the nerdie guy who sets up the machines? Do you trust the guys that programmed the software? Do you trust the (probably not native) guys who manufactured the individual computer chips? Do you trust the central computer that tots up the votes? Do you trust the guy in charge of that computer? Suddenly there are a lot of people you need to trust.

And its worse than that. The whole set-up is riddled with potential single-points-of-failure. The most devastating target for an attacker is clearly that central computer. Hack that and you decide the outcome of the election.

(I always recall the moment when a colleague of mine after just an hour or two of hacking our proposed Irish central computer system, turned to me and asked “OK Mike, who do want to win the next election?”. He wasn't kidding.)

In our manual system each paper vote in placed in a big black box. These boxes are place on the back of a truck where they are taken to the count centre with a police escort. The boxes are emptied on the tables, where an army of civil servants (who get the day off their normal duties) start bundling up the votes for each individual candidate. All of the while the agents of the candidates are only a few feet away watching the whole process.

Its actually a classic example of the power of **distributed trust**. Consider the problem of organising a conspiracy to subvert the manual system, without detection. Where do you start?

In fact the manual system can be subverted in some small ways. The classic Irish approach has been “personation”, whereby one voter votes in place of another. (True story - a friend of mine gets up late, rushes to the polling station, to be told by a neighbour emerging already - “Don't worry Mary – you have voted already”). A more dangerous attack is where the people in charge of a polling booth, after it closes, go through the voters register and vote for all of the people who didn't turn up to vote. This is called “voting the register”. But that requires a conspiracy involving multiple people, skews the turnout statistics, and is hard to go undetected.

In fact our manual system is extraordinarily robust against attack. It has the complete trust of the population.

So we need a dose of humility. Don't dismiss a manual system, instead learn from it and try and mimic its properties using technology. Don't go with any solution that places trust in any single centralised entity. Always distribute trust to the maximum extent possible.

I am confident that once we approach the problem in the correct way, we can use technology to assist in the voting process, in a way that gains the trust of the population. A lot of good research is going on right now. But we need to approach the problem with the right mindset.

Starting with this principle – always **distribute the trust**.