Robert Donovan
Edmonton
Alberta

20th September 2016

In my thirty years of computer system development experience I have discovered two very simple maxims. If you can't measure it, then it did not happen. Secondly, if the worst can conceivably happen, it will. Thus when I develop computer systems, I will embed various traces, records, and audit trails that will allow for my, and my customers' ability to trace what exactly has happened as the data flows through the system.

Yet, these systems are typically not perfect. The ideal is that my measuring system will identify and highlight any errors allowing me to deal with the issue proactively and quickly. Still errors happen and it is usually my customers, or their customers who identify the problem. To use an example of an organization that is nearly 100% data driven, I will use a bank.

The customers of a bank largely look at a simple measure of the data integrity of the bank's system; which is their account balance. Most bank users have a fairly good idea of what their balance should be, and the moment this diverges from what they expected they will begin looking through their transaction records to identify where their reality and the bank's version of reality diverge.

Often it is a forgotten transaction or some other simple issue, but other times it could be a system error or even fraud. The customer will bring this discrepancy into the bank and the issue is usually quickly resolved.

This bank example brings up two salient issues that directly relate to the feasibility of online voting. First is that by the nature of any online voting system the votes vanish into the system. A voter is unable to later "audit" the final status of their vote. It just disappears into a pool, much like a terrible bank that didn't separate their customer accounts but just let all their customers pool their money in one giant account, and to make matters worse kept no transaction records. Just one giant gelatinous balance.

The second issue that banks are fantastically secure institutions. They spend vast amounts of resources preventing, defeating, and mitigating the highly sophisticated attacks that such a valuable resource attracts. Yet very frequently they lose. Money is stolen, misdirected, or otherwise obtained in vast quantities by various bad actors. This same statement can be made about all of the other top end data institutions in the world. Facebook, google, ebay, paypal, microsoft, etc are all regularly hacked, with often serious breaches. These institutions are staffed by some of the smartest people on the planet.

Again what is doubly relevant is that it is often the end user who detects these attacks because of their ability to self audit their data. A bank account with missing money, a google email account with strange emails. A paypal account with mysterious purchases.

So as a person with decades of computer system experience, I can say that online voting has two fundamental weaknesses, the first is that like the banks, it can be hacked; to say otherwise is the statement of a con-artist or a fool. If the banks and companies like google can not prevent hacks then, very simply, nobody can prevent a hack. Thus the first and absolute assumption is that any online voting system will be hacked, full stop. The second is that the users affected by the hack will be unable to audit the system by later ensuring that the vote they cast is the vote that was counted. By its very nature, a successful hack is one that has bypassed the safeguards of the system, and thus any "detection" systems within the system cannot be trusted to somehow stand in for the millions of interested parties. A properly compromised voting system will happily give the proper thumbs up to anyone checking on it veracity and integrity.

Online voting has a secondary problem to the above which is the far narrower group of people who can be the bad actor, or potentially be induced to be a bad actor. Any one of the lead programmers can alter the system so that the outcome is determined by the person or small group of conspirators. There is a contest called "The Underhanded C Contest" where the goal of the competition is to write a program that clearly does one thing, while actually doing an evil other thing. In a recent contest the goal was to fool inspectors to the state of nuclear material. The submissions would easily pass most code reviews looking for malicious code. More importantly a small group of conspirators could easily "audit" each other's code entirely circumventing any such safeguard. A similar argument applies to any outside bad actors, in that they need not be a large group of people. Such deeds are regularly done by tiny groups of people.

I like to contrast this to how to perpetrate fraud in a traditional paper election. With thousands of ballot boxes, tens of thousands of election officials, scrutineers, and the people running for election. There are simply too many sets of eyes, and too large a conspiracy needed to properly swing an election. It would take sleight of hand magicians in thousands of polling stations, all successfully pulling off their ballot swaps, with none getting caught, and none of them spilling the beans.

Then to make this all even more interesting, I can use a very topical example of the "state of the art". Recently the NSA was hacked (not Snowden but a proper outside hacker) and a huge amount of their hacking toolkit was stolen. The thieves are presently trying to sell it for some Dr. Evil amount of money showing that even the vaunted NSA was partially an aura of security theatre. From what I have seen, all electronic voting systems have been held as closely guarded proprietary systems. Without exception, every single electronic voting system that was exposed to genuine, independent security researchers was completely debunked as worthless, insecure, and open to a significant number of easy attacks. Claiming that a system is secure is garbage. Proving it is secure to an adversarial group of experts is better, but like the experts at any bank will tell you, still not enough. Exposing it to experts will probably prove it to be garbage, but experts who claim it is secure simply indicates that they are biased, or not experts.

But the worst part of all of the above, is that the type of person who will (not might) be elected through this sort of fraud is exactly the type of person we don't want holding elected office. I see three paths to this type of election disaster. The first is simple lust for power. Someone will at best use an end-justifies-the-means rationalization, and engage in this sort of fraud. Second is that a party or backroom sponsor will support their candidate through fraud. And third is that some nation-state, or corporate sponsor will either prevent a toxic-to-them candidate from being elected, or will support a candidate who is favourable to them. In these last two examples, the winning politician in question may be an unwitting pawn.

Without a doubt there are various parties in the above categories who will have no moral reservations, and easily no resource problems to engage in such election rigging.

Quite simply, it cannot be prevented, and by the nature of any electronic voting system, cannot be identified in a smoking gun category way if the fraud is properly perpetrated. There may be "statistical" aborations, but not sufficient to allow a judge to nullify a result.

Keep in mind that online voting is a one way mistake. Once an election is won through fraudulent means, the people elected will certainly maintain the system that allowed them to win. At best the only party capable of taking the throne at this point is a group even more underhanded than the last.

Why would we risk one of the most important things that western civilization holds dear? For a bit of savings on ballot papers? To entice a few apathetic voters who couldn't be bothered to go to a polling booth? Plus, as an expert in computer systems, I don't see this as a risk, but a certainty; Google will be hacked, Apple will be hacked, facebook will be hacked, CIBC will be hacked, and any online voting system created by people with far less talented will certainly be hacked. The other hacks might cost me a few dollars or my email account. This hack will cost me my freedom.

Sincerely,

Robert Donovan