Online voting is convenient, but if the results aren't verifiable it's not worth the risk

May 14 2015, by Mark D. Ryan And Gurchetan S. Grewal

Credit: AI-generated image (disclaimer)

In one of the most fiercely contested elections in years, the turnout of the 2015 British general election was still stubbornly low at 66.1% – only a single percentage point more than in 2010, and still around 10 points lower than the ranges common before the 1990s.

There has been all manner of hand-wringing about how to improve voter engagement and turnout. Considering the huge range of things we now do online, why not voting too? A Lodestone political survey suggested that 60% of respondents said they would vote if they could do so online, and this rose to around 80% among those aged 18-35. As recently as this year, the speaker of the House of Commons called for a secure online voting system by 2020.

But designing a secure way to vote online is hard. An electronic voting system has to be transparent enough that the declared outcome is fully verifiable, yet still protect the anonymity of the secret ballot in order to prevent the possibility of voter coercion.

End-to-end verifiability

Any online voting system has to arrive at its conclusion in such a way that voters and observers can verify the count, independently of the software used – this is called end-to-end verifiability. This way voters can be assured that their votes were recorded as they were cast, and that all cast votes were counted correctly.

The vital nature of this can be explained by analogy to online banking. Bank customers can verify their own bank statements – and need not care about the software that produced them. But what if the banks provided no evidence of your transactions, just your remaining balance – how could you verify that the bank wasn't cheating you?

The difficulty in respect of online voting is that how each voter cast their vote must be kept secret – we can't just have a huge banking-like "statement" recording who voted which way. Instead, all the votes cast are gathered together and presented on a website in encrypted form, in order to ensure ballot secrecy.

The challenge is to design a way of using encryption that allows an independently-verifiable tallying of individual votes, without removing the secrecy it affords the ballots. Methods have been invented that allow the voting server to generate cryptographically-sound proofs that its count is correct. This means voters, observers and media organisations can perform the necessary checks to establish that the declared outcome really does match the votes cast in the elections.

Electronic voting in the real world

Online voting has been carried out eight times in Estonia, first in a local election in 2005 and, most recently, for its parliamentary elections in 2015. However the system Estonia uses does not support end-to-end verifiability. The tallying done by the server could be easily rigged, for example if someone has attacked the server with malware.

Norway also ran a trial of internet voting during local elections in 2011. The Norwegian system didn't support end-to-end verifiability either – and in fact Norway has ended the project amid concern it could damage confidence in the electoral process. Nor has online voting in either country boosted voter turnout. There are benefits to electronic voting – verifiability, lower cost, speed – but on the real world evidence so far boosting turnout isn't one of them.

We have recently seen researchers show how various attacks on existing electronic voting system are possible. Examples include iVote online voting system used in NSW elections in Australia or AVS WinVote machines used in three presidential elections in Virginia in the US. These attacks can affect the outcome of the election in an undetectable way, as there is no way for observers to verify independently the outcome of the election.

A system called Scantegrity was used in Takoma Park city municipal elections in the US in 2009, and vVote (an adaptation of the Prêt à Voter system) was recently used in Australian state of Victoria elections. These systems include mechanisms for end-to-end verifiability and so provide high assurance in the election results. But they are designed to be used in polling stations only, and so defeat the main perceived advantage of online voting by removing voters' ability to vote from anywhere.

The challenge of malware

Another challenge to designing verifiability in online voting is the possibility of malware infection of voters' computers. By some estimates between 30%-40% of all home computers are infected. It's quite possible that determined attackers could produce and distribute malware specifically designed to thwart or alter the outcome of a national election – for example undetectably changing the way a user votes and then covering its tracks by faking how the vote appears to have been cast to the voter. Whatever verifiability mechanisms there are could also be thwarted by the malware.

One way to try to prevent this kind of attack is to make voters use several computers during the voting process. Although this is hardly convenient, the idea is to make it more difficult for an attacker to launch a co-ordinated attack across several computers at once.

Online voting is attractive because it promises convenience. But providing true end-to-end verifiability remains an enormous challenge. Governments and politicians should be aware of the risks, and the possible loss of confidence in the voting system if whatever system introduced is found to be flawed. Democracy is important – if voting is to be done online it must be done properly, or not at all.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: Online voting is convenient, but if the results aren't verifiable it's not worth the risk (2015, May 14) retrieved 18 April 2024 from https://phys.org/news/2015-05-online-voting-convenient-results-worth.html