Internet voting: coming to a computer near you, though more research is needed to eliminate the risks

By Democratic Audit

Internet voting could represent an effective way to improve the accessibility of voting, and contribute to an increase in electoral turnout amongst the young. But while the internet is sufficiently safe for conducting bank transactions, this is not yet the case for politically binding elections. However, with research into the areas of concern progressing quickly, that will not be the case indefinitely, argue ***Mark Ryan*** *and* ***Gurchetan S. Grewal.***

Internet voting has the potential to provide efficient elections with higher voter participation, better accuracy and lower costs as compared to the current manual methods. People who have used internet banking and internet shopping know the convenience provided by the internet instead of standing in queues. In the UK, shoppers spent on an average of 16% more money online per person in the year 2012 as compared to 2011. With the introduction of internet voting, governments and policy makers are hoping to increase voter participation in a similar fashion to internet banking and shopping. In a survey conducted by Lodestone, 60.6% of people overall said they are more likely to vote if they could vote online, and 81.7% of the 18-35 year age group.

For all its convenience, however, internet voting comes with challenges. The internet can be made secure enough for internet banking. But voting is different: it is not easy to put mistakes right if they are uncovered after the results of the election have been declared. Moreover, in voting the requirement of ballot-secrecy means we cannot record a full audit trail of a voter's activity. This tends to lead to systems that are complex, which in turn makes the usability of such systems questionable; average voters find them difficult to use in practice.

Can we trust the outcome?

One approach to ensure the correctness of internet voting systems is to verify the software they use. Unfortunately, however, it is notoriously hard to prove anything about software. An alternative to that is to allow voters and observers to directly verify the outcome of the election. Using this idea, a voter is able to check that her vote is recorded as cast; and any observer can check that the final outcome is the sum of the votes cast. Here, an analogy with banking is useful: bank customers can directly verify their bank statements, and need not care whether the software that produced them is correct.

To achieve outcome verifiability, all the votes cast are gathered together and presented on a public bulletin board (for example, a website). But the votes thus presented have to be encrypted, in order to satisfy ballot-secrecy. Therefore, academics have proposed encryption schemes that are designed so that they allow tabulation to be done `through' the encryption layer. Additionally, methods have been invented that allow the voting server to give cryptographic proofs about the correctness of its tabulation. This means that voters, observers and any international media organisations can perform the necessary checks that establish that the declared outcome really does match the votes cast in the elections.

This kind of transparent encryption scheme allows voters and observers to verify the outcome produced by back-end software. However, it does not deal with the possibility that specially-produced malware could affect the vote at the time it is cast on voters' home computers. Indeed, some estimates are that 30% or 40% of home computers are infected, and one has to assume that determined attackers could produce and distribute malware specifically designed to thwart a national election.

To mitigate this possibility, academics have invented a technique called "cut-and-choose" allowing voters to check if their computer has correctly encoded their vote. After the computer produces the encryption, the voter can choose to audit it, that is, to get the computer to provide the data that proves the vote is correctly encrypted.

Although they are clever and sophisticated, these methods have been criticised because they are hard for voters to understand and use. To address this, more direct ways of verifying the election outcome have been proposed in

which voters are allowed to cast trial ballots. The trial ballots are not counted in the final tally, but voters can check if they are correctly decrypted on the public bulletin board. This allows voters to establish trust in the entire voting process (from their home computer to the server).

The election outcome-verifiability overcomes the difficulty of verifying software and, therefore, it is sometimes referred to as *software-independence.* Cryptographer Ron Rivest says that *"a voting system is software-independent if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome."* Another term related to software-independence is end-to-end (E2E) verifiability: the voting process should be verifiable, starting from the voting phase to the tabulation.

If a voting system satisfies these properties and voters and observers verify election outcome, then voters need not worry about the software being used in the elections.

Can I be sure my vote is secret?

To ensure free and fair elections, ballot secrecy is another vital aspect. Indeed, academic research has identified a strong form of ballot secrecy, which is known as incoercibility, ensuring that voters cannot convince someone else about how they voted. This prevents them from selling their vote, or being forced to chose a particular candidate. Coercion is not an issue in traditional voting methods, because the polling booth provides a completely private place where a voter cannot be influenced by the coercer at the time of voting. In Internet voting, coercion could take many forms – voters could be coerced by a family member, an employer or by organized criminals.

Several proposals exist in the voting literature that allow coercion to be avoided, resisted, or be made evident in internet voting. One idea (embodied e.g. in a scheme called Civitas) gives voters an option to pretend that they followed a coercer's instructions, but in a way that the resulting coerced votes don't count in final tally. The system doesn't provide any data that allow a coercer to see if the voter behaved according to the coercer's wish or not. Although mathematically very elegant, the anti-coercion idea is difficult to realise. It ends up making voters perform tasks that are rather counterintuitive, and therefore many people consider such systems unusable in practice.

Many of the complexities in internet voting schemes proposed by computer scientists arise because of the tension between election verifiability ("transparency") and incoercibility ("opacity"). One way to mitigate this difficulty is embodied in a proposal called Caveat Coercitor, which makes coercion evident instead of trying to resist it. It uses algorithms that detect if any votes were cast under duress and discounts such votes from the final tally.

Where is internet voting for elections actually in use?

Some countries are already using internet voting for legally binding elections. In Estonia, it was first used in 2005 for local elections and in 2007 for parliamentary elections. Voters use Estonian ID cards for authentication, which is a mandatory national identity document. To tackle coercion, only the last vote cast by a voter counts, and if a voter chooses to go to a polling station, then the vote cast in the polling station overrides any vote cast using the internet. Norway also ran a trial of internet voting during the local elections in 2011. The elections held in these countries show how internet voting could be used for large scale national elections, but the systems used in those elections only satisfy properties that are weaker than those we discussed earlier. The Estonian and Norwegian voting systems do not provide end-to-end outcome verifiability, as voters and observers need to trust some components of the system. A coercer could also deceive the coercion mitigation techniques used in them.

Another system called Helios has been successfully used in elections where coercion is not considered to be a serious concern. Université catholique de Louvain in Belgium has used it for electing the president of the university. The International Association for Cryptologic Research (IACR) also ran mock elections using Helios in 2010. This system gives anyone the ability to audit elections. It takes reasonable steps as well to preserve voter privacy.

Problems like coercion and vote buying are difficult to avoid in internet voting and therefore some electronic voting systems have been designed to be used in polling stations. End-to-end verifiable voting systems like Prêt à Voter and Scantegrity are used in controlled environments (polling stations); this enables them to give stronger

security guarantees compared to internet voting systems. The Victorian Electoral Commission (VEC) in Australia is implementing a system based on Prêt à Voter, which will be used in Victoria's state election in 2014. The polling station voting systems do satisfy software-independence and some incoercibility but polling stations are an intermediate step. Similar to internet banking, the goal is to move to internet as it is convenient and cost efficient.

What's expected in the near future?

Conventional wisdom used to hold that internet voting won't be secure because voters' computers themselves aren't secure. However, some countries have already started using internet voting with voter-initiated auditing where computers prove to voters that votes are properly encrypted. Some of those voting systems still do not satisfy software-independence and incoercibility, as the challenge of home computer being an uncontrollable environment makes this difficult.

From a security point of view, some more research is needed to completely solve the problem of coercion and improve usability of internet voting systems. Until that is achieved, it is difficult to consider internet voting secure enough for politically binding elections. However, researchers are making progress quite quickly and based on the techniques developed recently we are optimistic that internet voting would become a reality fairly soon.

—

Note: this post represents the views of the authors and not those of Democratic Audit or the LSE. Please read our comments policy before posting. The shortened URL for this post is: ***http://buff.ly/M6dvef***

—

Mark Ryan is Professor of Computer Security at the University of Birmingham's School of Computer Science.

Gurchetan S. Grewal is a Doctoral Student at the University of Birmingham's School of Computer Science