Voting for online democracy

May 6 2005

The Internet may be used to power elections in towns, cities, countries, and even across Europe thanks to the work of a recently completed project. It would mean voters could cast their ballots at home, in the street via mobile phones, or even when in another country.
That's the promise of e-Vote, an IST programme-funded project that drew together experts in systems design and analysis, computer programming and high-grade security.

The project successfully developed a secure, scalable, Internet voting system that is significantly more advanced than other products, according to Gorm Salomonsen, a senior systems engineer at Cryptomathic, one of the project's partners. It contains new security features not present in systems used in the US and tested in Europe. Furthermore, e-Vote developed a system that uses the Internet as its ballot box, while preventing a number of attacks. Currently votes in most virtual voting systems are cast in polling stations, just like the traditional ballot box. Concerns remain, primarily about coercion, phishing attacks and spyware attacks. Solutions for much of this exist, but are currently not included in the system.

The problems with e-voting

E-Vote stands to make democracy a much simpler and reliable political system, if it can overcome some of the problems with electronic voting.

Those problems are daunting. Designing a secure and reliable electronic voting system is a huge challenge. The e-Vote system must cope with a

bewildering array of potential electoral chicanery: impostors, double voters, and enforcers.

But the system must also cope with the new, online threats like hackers, spoofers, or identity thieves. While security is paramount, so is privacy. It is easy to intimidate voters if you can check on how they voted.

Finally, in order to be truly useful, the e-Vote system must be adaptable and scalable. It must cater for everything from corporate governance, through national elections to continental elections.

Even closed, proprietary systems installed at the polling stations like the traditional polling booths are prone to problems and accusations of fraud or lost votes. With proprietary systems only the makers know how it works. “That's not good for democracy," comments Salomonsen.

He believes any widely adopted electronic voting system should be open to expert, independent analysis to ensure that it cannot be compromised.

The promise of e-voting

The virtual vote remains an enormous challenge, but the potential benefits are even greater. For a start, it could enable larger turnout at elections. Currently a number of countries have problems of low turnout at elections. Such abstention rates undermine the validity of the poll and the ideals of democracy itself.

Second, it could cut the costs and increase the reliability of elections, if all the safety concerns can be met. Third, it could provide a near instant result after polls close. The e-Vote project members believe their system meets these challenges.

Here's how. The voter receives a password, currently via the postal

network just like a ballot in a normal election. The voter goes online and uses the password to access the site. Once there he or she can get any amount of information on the candidates before voting, another advantage of the system.

When the voter enters the password, a one-time 'digital signature' is issued using public key infrastructure (PKI), a well established and robust security protocol. This establishes the identity of the voter. The voter casts the vote.

In the background, the vote is encrypted using homomorphic encryption. This type of encryption allows the 'votes' to be counted without decrypting individual votes. Furthermore, each vote is authenticated using PKI and a zero-knowledge proof of correctness of the vote is attached. A zero-knowledge proof means a mathematical proof that an encrypted vote is the encryption of a valid vote.

"Our project was lucky in the sense that the homomorphic encryption technology became efficient enough just as we started developing e-Vote," says Salomonsen.

The system is not infallible. A weak link in the chain is sending the unique password to each voter. But that's a problem that also exists with regular postal voting, without any of e-Votes' other advantages.

Furthermore, as electronic voting becomes more widely accepted and the electorate is educated in its use, it will be much more difficult to intercept posted passwords without alerting an aware electorate.

e-Vote on trial

Last year, e-Vote's system was validated in a series of small-scale trials, involving up to 2,000 voters, and it performed well. "We did run into

some problems," says Salomonsen. "In Slovakia, for example, we ran two plebiscites with about 2,000 people, but because broadband is not widely available there it took a long time to download to upgrade/install the JAVA virtual machine to run the applet that encrypts the vote."

"Right now it's better for broadband countries, but we are continuing development. Besides, for now we customise the system on a case-by-case basis, depending on the needs of a particular customer," he says.

Project partner Quality and Reliability, a Greek firm, are currently trying to commercialise the software and Salomonsen says that interest is high in small municipalities. "That's where we need to start with this technology," he says. Ultimately he believes the electronic voting market could be worth 1 billion euro a year.

There are risks related to electronic voting, and promoters of the concept are aware of these. But the risks are well worth the gain in a political system that is undermined by the very lack of citizen participation: e-Vote will, via its Internet platform, potentially enable larger participation in elections in a secure and reliable fashion.

Source: IST Results

Citation: Voting for online democracy (2005, May 6) retrieved 26 April 2024 from https://phys.org/news/2005-05-voting-online-democracy.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.