PHYS.ORG

Online voting a step closer thanks to breakthrough in security technology

April 30 2015

Credit: George Hodan/Public Domain

Researchers at the University of Birmingham have developed a technique to allow people to cast their election vote online - even if their home computers are suspected of being infected with viruses.

Taking inspiration from the security devices issued by some banks, the security and privacy research group at Birmingham, led by Professor

Mark Ryan, has developed a system that allows people to vote by employing independent hardware devices in conjunction with their PCs.

The new technique offers a fresh contribution to the debate surrounding e-voting and could be ready for use in time for the 2020 or 2025 General Election.

Professor Ryan said: 'This system works by employing a credit card-sized device similar to those used in online banking. It is called Du-Vote, and we have been developing it over the past two years. From the voter's perspective, it's straightforward: you receive a code on the device and type it back into the computer.

'The main advantage of this system is that it splits the security between the independent security device and a voter's computer or mobile device. A computer is a hugely powerful, all-purpose machine running billions of lines of code that no one really understands, whereas the independent security device has a much, much smaller code base and is not susceptible to viruses.'

Online voting carries a strong security requirement because of the possibility of undetectable interference in an election by foreign governments, criminal gangs, or petty fraudsters. Malware affects an estimated 20% to 40% of PCs globally, and specific election-targeting malware could be developed to attempt to alter votes cast or compromise ballot secrecy.

Gurchetan Grewal, who is part of the project team and recently completed a PhD in online voting at Birmingham, said: 'This is currently the only piece of work that addresses a core problem of e-voting - namely, that someone may have viruses or other malware on their computer. For example, the system in Estonia, where they have already introduced online voting, does not deal with this potentially undetectable source of vote manipulation or breach of voter privacy.'

The system being developed at Birmingham aims to bypass and detect malware by using a separate security device. But the system achieves even greater security than those used by banks by allowing for the possibility that the security devices themselves have been manufactured under the influence of a hostile adversary.

Paradoxically, the researchers succeed in proving that even if a hostile adversary controls the entire computing infrastructure, voters and election officials can still detect electoral fraud.

The research paper, titled 'Du-Vote: Remote Electronic Voting with Untrusted Computers', will be presented at the 28th IEEE Computer Security Foundations Symposium in Verona, Italy, in July.

Provided by University of Birmingham

Citation: Online voting a step closer thanks to breakthrough in security technology (2015, April 30) retrieved 10 April 2024 from https://phys.org/news/2015-04-online-voting-closer-breakthrough-technology.html