UK COMPUTING RESEARCH COMMITTEE

UKCRC/2014/4

Speaker's Commission on Digital Democracy
Consultation on Electronic Voting

UKCRC Response

The UK Computing Research Committee (UKCRC), an Expert Panel of the British Computer Society (BCS), the Institution of Engineering and Technology (IET) and the Council of Professors and Heads of Computing, was formed in November 2000 as a policy committee for computing research in the UK. It includes about 115 individual members, who are leading computing researchers each having an established international reputation in computing. Our response thus covers UK research in computing, which is internationally strong and vigorous, and a major national asset. This response has been prepared after a widespread consultation amongst the membership of UKCRC, and as such is an independent response on behalf of UKCRC and does not necessarily reflect the official opinion or position of the BCS or the IET.

This consultation is concerned with electronic voting and asks a number of questions about online voting. These two topics are different, and each should be considered on its own merits. This response distinguishes two types of electronic voting as follows:

Local (supervised) voting: the electronic capture and processing of votes where the vote is cast under supervised conditions in polling stations on equipment provided by the election authorities.

Online (or internet, unsupervised) voting: voters cast their vote from their own device or computer, submitting it remotely via a network to an election server which collects and then processes the votes.

Introduction of electronics into either of these two types of voting system introduces new risks compared to paper-based elections, since the electronic processing of votes is not directly visible in the way that paper ballot processing is directly visible.

The particular challenge for voting systems is that all votes are secret, and the expected result of the election is not otherwise known, so there is no independent check on the result returned by the system. The integrity of the process is thus central to the integrity of the result. This is unlike almost any other form of computerised activity, such as banking, where the result of a transaction can be checked, and so mistakes and fraud can be identified and corrected. Furthermore, banks bear the cost of fraud and breaches of security that they suffer. In the case of electronic voting systems it will be the voters who bear the cost of fraud, and they may not even be aware that it has occurred. Hence the most important question for any new election technology is not whether local or online electronic voting is possible, but rather the security question:

- *Can system errors or malicious attacks from insiders or external attackers undetectably change the result of the election or compromise the secrecy of the ballot?*

Currently, our view is that we do **not** yet have the technology to achieve fully usable and sufficiently secure electronic voting systems. In the last two years, the world has learned that powerful nation-state actors are perpetrators of some of the most severe Internet threats. Examples include Stuxnet, surveillance programs and cyber attacks on enterprises and government agencies home and abroad. Any country deploying online voting faces the possibility that the outcome of their election will be determined by another hostile state. As we cannot currently mitigate risks associated with online voting with sufficient confidence in the context of today's Internet threats, we recommend that **with current technology, online voting should not be used for statutory political elections at this time**.

Nevertheless, research on electronic voting (including online voting) is being pursued by research groups around the world, and the academic literature is evolving fast. It is likely that research done over the next decade or so will produce systems that satisfy the stringent properties (particularly the property of end-to-end verifiability) that electronic voting demands.

What are the potential benefits and drawbacks of online voting (eg, voting via the internet using a computer or mobile device)?

Online voting presents significant security risks, some of which we list here.

1. Online voting currently provides no way to independently audit or recount the votes, or to provide assurance that the vote has been received, stored and processed correctly, though research on "end-to-end-verifiability" (see below) may provide an adequate solution
2. Attacks on election servers may be undetectable because there is no externally independent record of the election data. Votes might be invisibly altered, by insider fraud or external attack. Again, "end-to-end-verifiability", is a potential solution to these problems
3. Voters' devices are vulnerable and almost impossible to secure. They can be subject to malware and virus attacks (e.g. the 2012 Zeus virus), which could provide the capability to invisibly steal or alter votes.
4. Online election servers may be vulnerable to cyber-attacks such as denial of service attacks, or penetration and vote-tampering. They are also vulnerable to insider attacks. Attacks on well-known highly secure sites of major organisations including banks and commercial sites are reported with alarming regularity. Election systems provide a very high-stakes target, and there is no reason to expect that election systems are any more secure than others that have suffered attack.
5. Software bugs could change the outcome of an election, with no way of proving that the declared candidates were wrongly elected.
6. Voting from a private device in an unsupervised environment potentially enables vote buying and selling and coercion of voters, and provides no guarantee that the vote is provided by the claimed voter. This would be the case even for a fully secure voting system.
7. Voters can be subject to social engineering or phishing attacks to reveal their credentials or to have their vote captured by a fake website.
8. Any special equipment (e.g. a dongle or cryptographic keypad) needed for online voting will be infrequently used by voters. Vulnerabilities may arise through lost and stolen items, as well as forgotten passwords and PINs.

The consensus among computer security experts and electronic voting researchers is that online voting is currently unsafe. For example, the `Dagstuhl Accord' of 2007 signed by 21 researchers attending the Dagstuhl Conference on Frontiers of E-Voting, agreed that:

> *Voting over electronic networks has various attractions, is starting to be deployed, and is regarded by some as inevitable. No solution, however, has yet been proposed that provides safeguards adequate against various known threats. Problems include attacks against the security of the computers used as well as attacks that impede communication over the network. Improper influence of remote voters is also a significant problem, although it is tolerated with vote by mail in numerous jurisdictions. Securing network voting is clearly an important research challenge. We cannot, however, prudently recommend any but unavoidable use of online voting systems in elections of significant consequence until effective means are developed to address these vulnerabilities.*

The concerns raised then remain current today. More recently, in December 2012, an open letter to President Barack Obama had 51 signatories encompassing elections officials, experts in cyber security, election law, post-election audits, election integrity, and accessible technologies. The letter included the following paragraph expressing opposition to Internet voting:

> *Internet voting (the return of voted ballots over the Internet including fax and e-mail) has been proposed as a solution to long lines at the polls. But since it is vulnerable to attacks from anyone/anywhere, Internet voting must not be allowed at this time. In addition to security and accuracy risks, Internet voting threatens the secret ballot, which is key to avoiding voter coercion and vote buying and selling. The secret ballot was originally instituted not as a right that an individual can waive, but rather as an obligation of the government to protect all citizens from coercion and intimidation as they cast their votes. Because of multiple intrinsic risks, Internet voting should be forbidden unless and until proposed systems have undergone extensive, independent public review and open testing to ensure that they have solved the fundamental problems of security, privacy, authentication, and verification.*

All these arguments refer to the technologies that have been developed so far. But researchers around the world are working to develop new methods, and the topic of electronic voting is evolving fast in the academic literature. It is likely that research done over the next decade will produce systems which are able to satisfy the stringent security properties that electronic voting demands.

What impact, if any, would online voting have on voter turnout?

Insufficient research has been carried out to date on this question. The recent trials in online voting in Norway (2011, 2013) concluded that turnout was not increased by online voting. The February 2014 Recommendations Report to the Legislative Assembly of British Columbia reached a similar conclusion, stating (p 12)

> *While there have been some Internet voting elections where voter turnout has increased, when other factors such as the apparent closeness of the race and interest in particular contests (e.g., a mayoral election without an incumbent) are taken into consideration, research suggests that Internet voting does not generally cause non- voters to vote. Instead, Internet voting is mostly used as a tool of convenience for individuals who have*

already decided to vote.

It also states (p 13):

> *Researchers have also looked at the demographics of Canadian voters who have used Internet voting and have found that Internet voting is most popular among middle-age voters and least popular among youth and therefore reflects traditional voter turnout demographics. These findings run contrary to the widely expressed belief that Internet voting will lead to increased participation by youth.*

Would online voting increase the 'digital divide' or increase accessibility in elections?

Electronic voting has the potential to provide improved accessibility for voter groups who would benefit from electronic assistance in completing a ballot form or casting a vote, including blind, partially sighted and motor impaired voters, and those who cannot read English. Accessibility can be improved by the provision of a computer with a suitable user interface to capture the vote. It is not provided by online voting specifically.

However, it is important to note that accessibility is not automatically provided by electronic voting. Care must be taken to design interfaces that conform to accessibility standards such as the Web Content Accessibility Guidelines WCAG 2.0, and any proposed system must be required to meet such a standard.

What are the cost implications of online voting?

The initial costs of creating a system are likely to be high, because security done properly is not cheap. However, as with banking, shopping, communication (all of which have gone online in the last few years), it is reasonable to expect that the costs of running elections will reduce if they are put online.

What are the advantages and disadvantages to using electronic voting machines in polling stations instead of paper ballots?

Advantages of introducing electronic voting machines into polling stations include:

1. accessibility for blind, partially sighted and motor impaired voters through custom user interfaces;
2. the opportunity to present the voting interface in a variety of languages;
3. guidance through the voting process and a consequent reduction of accidentally spoiled ballots, particularly for unfamiliar instructions;
4. the ability to collect votes promptly from overseas locations (e.g. embassies);
5. the collection of votes in electronic form can enable faster and more accurate tallying of the result;
6. savings on the cost of printing paper ballots.

Disadvantages include:

1. the challenge of building a system in which manipulations of the outcome by an attacker are detectable by voters and observers. In the literature, this is called "end-to-end verifiability".
2. the challenge of obtaining and maintaining public trust in a system whose internal workings are not well-understood, especially if there are early problems in introducing a system;
3. the need for robust system and procedural security

Would electronic voting at the ballot box be a useful step towards online voting?

We do not consider online voting to be an appropriate option at present. From a technological point of view, electronic voting in supervised polling stations under controlled conditions should not be considered as a step towards online voting, because the methods that are developed for poll-station voting are not the same as the ones needed for online voting. However, from a sociological point of view, poll station voting could be a useful stepping stone in order to allow voters to get used to the technology. It can help voters get used to the verifiability requirements that they will later encounter in online voting.

What can be learned from e-voting experiences in other countries?

Internationally, online voting for national elections is rare, though some countries make it available for particular groups of voters (e.g. overseas voters; military). Supervised electronic voting is more common. In all cases it is clear that security is a major consideration.

Internet voting

Estonia has allowed voting over the Internet since 2007 (following a pilot in 2005). The Estonian system relies on the strong e-id national infrastructure to underpin voting over the Internet in advance of polling day. It allows voters update their vote (as a defence against coercion). The OSCE/ODIHR Election Assessment Mission Final Report for the 2011 Parliamentary election made several recommendations, including greater transparency and verifiability, and improved controls over the version of the software running during the election. In 2014 security concerns were raised about the system by computer security experts, the possibility of a malware attack has been demonstrated, and poor security practices have been identified. No attacks against a real election have been reported.

Norway ran trials on Internet voting in 2011 and 2013 but has since decided not to continue. They found that voter turnout did not increase. Furthermore, in the 2013 trial a coding error resulted in the potential loss of vote privacy for approximately 29,000 voters.

The Australian state of New South Wales ran an internet voting system in its 2011 state election. Voters were told at the time that their electronic receipt number “confirms there has been no tampering to the vote”, but this description was not at all accurate. A security audit found “significant security vulnerabilities,” of which some “remained outstanding during the voting period.” Of the 44,605 votes received over the Internet, 43 were invalid because they contained the letter ‘N’ instead of preference numbers, due to a programming error. The election commission intends to rerun Internet voting, using a new system from a different vendor, in the upcoming 2015 state election.

In 2010 Washington D.C. ran a pilot project to allow Internet voting for overseas and military voters, and invited the public to test the system shortly before deployment. A team from the University of Michigan penetrated the system within 36 hours and gained almost total control of it, enabling them to change votes and to see voters' secret ballots. They demonstrated that a malicious attacker would have been able to manipulate the election outcome without detection.

Supervised electronic voting

A wide variety of electronic voting systems are run across the U.S., since each jurisdiction has autonomy in running elections. In 2007 the Secretary of State for California, Debra Bowen, commissioned a `top to bottom' review of the voting systems certified for polling place use in California. Security experts reviewed the source code (the programs running the systems) and carried out penetration testing (seeking ways to attack the systems). They found significant security flaws in all the manufacturers' systems they reviewed, resulting in decertification of the systems and stringent conditions for recertification.

One widespread feature of electronic voting in the U.S. is the use of paper records to address the concern that Direct Recording Electronic (DRE) voting machines process votes in purely electronic form. Open questions remain about the way this is currently done: how can this be done in such a way that the anonymity of the vote is guaranteed? How can the chain of custody of the paper trail be assured? More research is needed to resolve these questions.

Brazil has been using electronic voting on custom machines since 1996, and India since 1999. India has recently introduced the use of paper records as a pilot in the 2014 general election, to address concerns that the voting machines are not tamper-proof.

What safeguards would be needed to reassure the public that their digital vote was secure?

End-to-end verifiability: The ideal would be to provide independently auditable evidence that the election has been conducted correctly. Reassurance will be obtained from *end-to-end verifiability*: that voters can check their votes have been correctly included in the count, and that the votes have been correctly tallied. There are ways developed in the academic literature of achieving verifiability of the election outcome while maintaining ballot secrecy, using verifiable cryptographic techniques. Examples of systems with this verifiability property include: JCJ (2005), Pret-a-Voter (2005), Helios (2008) and Scantegrity (2008). Other proposals (and refinements of these ones) have also been made. However, combining verifiability with anti-coercion properties and user-friendly interfaces remains a challenge.

Transparency: Election systems code is complex, and is often proprietary and closed. Making election systems code and documentation open to security and electronic experts and the public for analysis and review would provide some confidence in the expected behaviour of the system. Openness does not automatically ensure that the system is correct or secure, but the opportunity for external scrutiny allows for vulnerabilities and bugs to be identified and corrected, and enables well-informed discussion about the technical properties of the system.

Malware tolerance: the ability to use computers and devices reliably even if they have been infected with malware. This is not available with existing technology, but it is an active research area and is likely to be available within five to ten years.

Would it be possible to guarantee the integrity of the ballot?

Guaranteeing integrity of the ballot for online voting is extremely difficult with current technology for the reasons given above. This is an area of active research, and advances in technology may make this possible in the next ten years.

There are supervised electronic voting systems that provide end-to-end verifiability. These give a cryptographically secured audit trail of the processing of the votes, providing evidence of the ballot's integrity. Verifiability includes the ability for voters to check that their votes have been recorded as cast, the ability for independent observers to check that all recorded votes have been tallied correctly, and the ability for independent observers to check that only eligible voters have cast votes. Any tampering of the election would be evident through the inconsistency of the published cryptographic record. A consistent record guarantees the integrity of the election. This is an important continuing area of research. A systematic evaluation of the various current approaches, with respect to their potential use in UK national elections, is highly desirable.