Electronic Balloting Review
Independent Review of Electronic Balloting for Industrial Action: Call for Evidence

Evidence from the UK Computing Research Committee.

July 14th, 2017

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. Its members are leading computing researchers who each have 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.

The committee has asked for input on 12 questions which we have addressed separately below.

Q1 What are the strengths and weaknesses of the current postal system for achieving the required standards?

The definite positive aspect of the postal vote is that it is simple to use; most people are familiar with the process and it requires very little effort to understand how it works. On the negative side, it has been argued that it is not sufficiently secure. For instance in a particular case related to Birmingham 2004 city council elections, the election commissioner stated, "The ease of postal vote fraud and the difficulty of policing it led to such a great upsurge in personation that, in the Birmingham case, the number of false votes was virtually half of all votes recorded as having been cast for the winning candidates."[1] Furthermore, it is also wide open to coercion, (as all remote voting systems are, in the absence of countermeasures); a special case of such coercion is family voting.[2] In the "Code of good practice in electoral matters" by the Council of Europe[3], the importance of protecting individual voting from coercion is highlighted.

[1] For more information see http://www.telegraph.co.uk/news/uknews/law-and-order/11560017/Postal-voting-fraud-is-easy-electoral-commissioner-says.html

[2] The issue of family voting is also discussed in E. Benoist, B. Anrig and D.-O. Jaquet-Chiffelle. *Internet-Voting: Opportunity or Threat for Democracy?*. In Vote-ID 2007.

[3] Council of Europe, 2002. Opinion No. 190/2002. For more information see http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2002)023rev-e

Q2 Please give examples of situations where you are aware e-balloting is currently applied. What type of technology is deployed eg Internet based, telephone-based? What has been the impact and how has it been evaluated

E-balloting is applied in several countries' binding elections at a municipality or national level (Belgium, Brazil, Canada, Estonia, India, Switzerland, USA). Perhaps the most prominent example is the case of Estonia that began using national internet voting (i-voting) in 2005, and has served in eight elections. In the 2005 local elections, only 1.9% of voters cast their ballot online, rising to more than 30%.[4]

A notable example of an association that replaced successfully postal voting with e-voting is the International Association for Cryptologic Research (www.iacr.org). The switch to the e-voting system happened in 2010 and it was a purely Internet-based solution. In 2010 they had a record high of participation jumping to 30% of the membership from the past where typically participation was around 20%.[5] The participation was maintained at this higher level in all the upcoming years as shown in the table below.[6]

2010	2011	2012	2013	2014	2015	2016
30%	41.8%	33.9%	38.6%	40.9	30.1%	34.7%

Based on the above numbers it appears that e-voting compared to postal e-voting increased participation significantly. The underlying system (called Helios voting) has been subjected to a number of security analyses.[7]

Other notable cases of successful use of internet based e-voting have taken place in Greece where binding university elections (for administrative positions of rectors, vice rectors and department heads) are regularly held nation-wide for all Greek universities with considerable success[8]. Internet-based e-voting has been also used by universities as a pedagogical tool.[9]

[4] See (http://www.bbc.co.uk/news/business-39955468). An improved version of the Estonian i-voting system that supports stronger verifiability was used in the 2013 Municipality elections and 2014 European parliament elections. The electorate's reception of the new system is analysed in Heiberg and Willmeson *Verifiable internet voting in Estonia*. In EVOTE 201

[5] See the web-site https://www.iacr.org/elections/2010/

[6] The data reported in https://www.iacr.org/elections/

[7]See e.g., Véronique Cortier and Ben Smyth (2011) Attacking and fixing Helios: An analysis of ballot secrecy. In CSF'11: 24th Computer Security Foundations Symposium, IEEE Computer Society, pp. 297-311 and Aggelos Kiayias and Thomas Zacharias and Bingsheng Zhang, Ceremonies for End-to-End Verifiable Elections, https://eprint.iacr.org/2015/1166

[8] This is achieved using the Zeus e-voting system see George Tsoukalas et al.: From Helios to Zeus. EVT/WOTE 2013 and https://zeus.grnet.gr/zeus

[9] For instance, Newcastle University uses an i-Voting system for classroom voting and student prize competitions since 2013, see Feng Hao et al., "Verifiable Classroom Voting in Practice," *IEEE Security and Privacy*, in press 2017. http://eprint.iacr.org/2017/056.pdf

Q3 How much do you believe the use of e-balloting for industrial action would increase turnout, if it were available? What other access benefits might it bring?

Evidence for general type of elections with respect to e-balloting has been quite mixed in terms of increasing voter participation. For instance in the case of national elections in Estonia there was no evidence of introducing new voters because of e-voting according to a study[10] while in Brazil a modest increase was exhibited.[11] For industrial action specifically, based on the data presented above for the IACR one might be more optimistic. However it should be stressed that the IACR members have relevant expertise and/or may feel more motivated and/or comfortable to use an e-voting system. Furthermore IACR is an international organisation with membership spanning across continents.

It is safe to say that an e-balloting system may enjoy a user-friendly interface that along with the feature of fast online vote submission (compared to mailing an envelope), would be preferable in terms of usability and accessibility to the election procedure for people that face special circumstances. In fact it is easy for the e-balloting system to be designed so that it can be personalised to the abilities of each voter individually. Furthermore, commercial electronic devices (PCs, laptops, tablets, smartphones) that can support secure vote casting are increasingly becoming more affordable and usable thus potentially narrowing the so called digital divide that might prohibit certain groups of people from using e-balloting. Another potential and general access benefit of e-balloting (to be elaborated also below) is the fusion between the voting system and deliberation tools such as online discussion forums and the capability to enable voters to perform direct auditing of the election result. If an end-to-end e-voting system is used for e-balloting, one further significant benefit is in ensuring that the ballots will be cast-as-intended, recorded-as-cast and tallied-as-recorded. In comparison, the current postal voting system can only guarantee the ballot is cast-as-intended; once the ballot is posted out, there is no way for the voter to verify if it will be recorded and tallied correctly.

Q4 Which forms of e-balloting system (eg telephone / internet) would help ensure access? What evaluations have taken place on the robustness and resilience of different systems to ensure access in a voting context?

If postal voting remains an option in conjunction to e-balloting, it would appear that participation and access would not be hurt; voters will still have the option to utilise the postal procedure if they prefer while e-balloting will provide another way to participate. However, it would be important to examine carefully the security implications of composing the two systems as it could be the case that the resulting hybrid system may not retain the same security properties as its two constituent sub-systems. Regarding accessibility, e-balloting systems may be designed to be more flexible in terms of their user interface and thus they can be more accessible to people with special abilities.

Q5 In what circumstances might e-balloting be more or less secret when compared to postal voting?

[10] D. Bochsler, Can Internet Voting increase Political Participation? Internet and Voting 2010.

[11] P. Spada et al., Effects of the Internet on Paricipaption, World Bank Group February 2015.

Generally speaking, both postal voting and e-voting can provide an acceptable level of ballot secrecy but are potentially subject to coercion. However, in the case of e-balloting special care needs to be applied when creating the cryptographic key information that is required to encrypt the votes. State of the art e-balloting systems utilise methods such as “distributed key generation” that ensure there is no “single point of failure” for the secrecy of the votes.

Any remote voting, either via post or electronic means, will be prone to coercion and vote-selling, if the election authorities cannot guarantee a moment of privacy and self-reflection as such provided by the deployment of a voting booth. The advantage of e-balloting on this front is that there might be special mechanisms that can be engineered into the system to allow a level of coercion resistance (see also Q7 below).

A point in favour of e-balloting is that via the use of efficient cryptographic techniques one can facilitate the electronic counting of votes in a collective way at a mass scale without ever revealing partial tallies. This allows for processing the votes in the largest possible sets, thus increasing the anonymity in terms of the size of the voter pool. In plain words one is more anonymous when they are one out of a million as opposed to one of a hundred. The issue of privacy compromise by the revelation of a partial tally when the voting takes place in small size groups is a well-known issue.

Q6 What mitigations can be employed to ensure that under e-balloting, hacking of the system, even if successful, would not allow the identity of a vote to be revealed? Have such mitigations been evaluated?

In the setting of e-voting systems there are several techniques to preserve the secrecy of the votes. In particular, advanced encryption mechanisms such as homomorphic encryption[12] has been demonstrated to be very useful in preserving the privacy of encrypted ballots while enabling the computation of the final tally. Another technique that has been successfully employed in the context of e-voting for anonymization of the submitted ballots is the use of a mix-net which is the electronic equivalent of shaking up the ballot box to mix up the votes, so no cast vote can be associated with any individual.[13] In terms of coercion, a number of techniques have been proposed to reduce the opportunity for coercion / intimidation in the context of e-voting, for example by allowing re-voting to overwrite an earlier vote or issuing voting credentials that do not contribute to the final tally (and may be shared with a coercer).[14] There has also been work on automatically identifying ballots that were cast as a result of coercion, and removing them.[15] Using such cryptographic mechanisms properly, the level of vote secrecy provided by e-balloting can be reasonably high, at least in theory.

Q7 Would e-balloting increase the scope for intimidation and undue influence (being forced to vote, and being forced to show which way someone had voted, and being forced to vote in a certain way)?

[12] The first time this was proposed is in J. Benaloh, Verifiable Secret-Ballot Elections, Ph.D. Thesis, Yale University, 1987.

[13] For the introduction for concept of mix-nets see, David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Commun. ACM 24(2): 84-88 (1981)

[14] For instance see Ari Juels, Dario Catalano, Markus Jakobsson: Coercion-Resistant Electronic Elections. Towards Trustworthy Elections 2010: 37-63.

[15] For example, see G. S. Grewal et al. Caveat Coercitor: coercion-evidence in electronic voting. In IEEE Symposium on Security and Privacy, 2013.

A number of recent research papers explore the domain of incoercible e-voting systems i.e., systems where it is not feasible for an attacker to exert coercion against the voters that participate in an election.[16] Combining these techniques with the ability to verify the final tally is a topic that requires further attention from a research point of view. On the other hand, comparatively speaking, intimidation is also an important concern in the postal voting case. Nevertheless, coercion might take different forms in the setting of postal votes and in the setting of e-balloting. For instance, in e-balloting one may be able to vote from a smart phone which is a device that someone brings at work. On the other hand, postal voting might more likely take place at home away from the office potentially reducing the possibility of coercion or peer pressure. A hybrid system may be considered where e-balloting credentials can be posted to a home address using the postal service but vote collection and tallying is done electronically. For instance, one countermeasure that has been applied against coercion in Estonian balloting elections is enabling the voter to submit multiple ballots where only the last one counts. This feature is easy to be supported in an e-balloting approach, whereas it seems significantly harder to achieve in the postal voting setting; it should be added however that re-voting may introduce other complications in the verification of the tally that need to be carefully evaluated before deployment.

Q8 How do you believe technology has evolved or will evolve to address the risks set out above?

It is evident that the computer science research community is well aware of many of the security issues related to e-voting. Despite successful adoption of e-voting systems in a number of instances there still appears to be no e-balloting system that solves all conceivable problems and there have been a number of concerns voiced against the use of e-balloting in national elections. On the other hand, for the problem at hand, potential e-balloting weaknesses should be compared and contrasted to the postal voting solutions since postal voting is also susceptible to a number of similar attacks. As always, introducing new technology does introduce new attack vectors and these need to be understood and mitigated. E-balloting systems, if designed poorly, can fail in a much more devastating manner compared to classical systems.[17]

From a general security perspective, upcoming and currently ongoing developments (e.g. the development of secure communications protocol TLS1.3) are expected to improve the security of internet connected devices which can be directly beneficial for the e-balloting case.

Q9 How will e-balloting change the scope for industrial action and how does that affect the public interest?

E-balloting can be easier and faster to execute, assuming people are properly trained for the system and they have a reasonable level of familiarity with PC/smartphone/tablet devices. As a result, a sequence of e-balloting instances can be run over short periods of time or even concurrently on different election

[16] See e.g., J. Alwen et al.: Incoercible Multi-party Computation and Universally Composable Receipt-Free Voting. CRYPTO (2) 2015: 763-780

[17] For an example of an ill designed e-balloting system and its susceptibility to a serious attack see Wolchok et al. Attacking the Washington DC Internet Voting System, In Proc. 16th Conference on Financial Cryptography & Data Security, Feb. 2012.

options. Furthermore, e-balloting can be directly combined with other tools such as online forums that assist union members deliberating and forming opinions about relevant union matters. Voting and deliberation can thus be considered to be part of the same platform hence streamlining the participatory process. Given the above, one might speculate that this enhanced flexibility can allow for a more active involvement of union members in consultations and hence an increased level of interest in union matters.

Q10 Are there other risks or challenges associated with e-balloting, not identified above? How might they be mitigated?

Denial of service is a critical concern in any system that runs in an open network such as the Internet. Selective denial of service is even more troubling in the case of an e-voting system since attackers may target a specific segment of the electorate thus biasing the election result. Denial of service issues are also in principle present in the postal voting case. Even though there are reasonable concerns regarding these attacks, denial of service is detectable in general and thus the attack may still be mitigated in some way (e.g., by rerunning the procedure or extending the ballot collection period). E-balloting introduces potential risk of tampering with votes systematically and at scale, and by a remote attacker. This risk is not present to the same degree in postal voting, where physical access to voters or ballot forms is required to attack the integrity of the vote. For this reason, it is important to adopt a principled approach in the deployment of an e-balloting system by suitably utilising mitigation techniques that have been developed by the e-voting research community. For instance, end-to-end verifiability has been put forward in the context of e-voting[18] to provide assurance against large scale fraud. Case studies showed favourable perception for verifiable elections even among older participants that are not particularly technologically savvy.[19] Removing possible single points of failure by deploying e-balloting over a fault tolerant distributed infrastructures is another important consideration that can be addressed by employing suitable techniques from distributed systems.

There is also the possibility that a well-funded foreign state adversary could try to interfere with industrial ballot elections, similarly to the alleged Russian hacking of the USA presidential election of 2016.[20] Industrial ballots are generally smaller scale and with smaller political significance than national political elections, and therefore the motivations may be lower. Nevertheless, interference in a larger scale industrial ballot (say of the size of the current Southern Rail industrial dispute) could significantly impact on the UK economy, and this could be sufficient to motivate foreign nation states. One vector through which such an attack could be perpetrated is by spreading targeted malware that specifically attack the voter's voting platform (e.g., their mobile phone or laptop), potentially changing the way they vote. Recent work in e-voting has considered how to detect and thwart such attacks[21], but further investigation

[18] See David Chaum (2004). "Secret-Ballot Receipts: True Voter-Verifiable Elections". *IEEE Security and Privacy*. **2** (1): 38–47. doi:10.1109/MSECP.2004.1264852.

[19] For an example of such a study see e.g., Pressing the button for European elections: verifiable e-voting and public attitudes toward internet voting in Greece. By Delis et al.. 6th International Conference on Electronic Voting: Verifying the Vote, EVOTE 2014 http://ieeexplore.ieee.org/document/7001141/

[20] U.S. government officially accuses Russia of hacking campaign to interfere with elections (Washington Post, 7 October 2016).

[21] For instance, see G.S. Grewal et al., Du-Vote: Remote Electronic Voting with Untrusted Computers. In 28th IEEE Computer Security Foundations Symposium (CSF), 2015 as well as the DEMOS line of e-voting systems that explicitly address corrupted clients in an end-to-end verifiability setting, by Aggelos Kiayias, Thomas Zacharias, Bingsheng Zhang, End-to-End Verifiable Elections in the Standard Model. EUROCRYPT (2) 2015: pp. 468-498, DEMOS-2: Scalable E2E

would be in general needed to ensure that accessibility and usability can be combined with these techniques.

Q11 How might other non-technological processes need to change, such as the role of the scrutineer, if e-balloting were made available for industrial ballots?

The role of all involved entities including the scrutineer would have to tie in with the underlying technology that is being used. For instance, a number of state of the art e-balloting systems support end-to-end verifiability and additionally have the capability to facilitate delegation to a third party for scrutiny.[22] In this way the role of scrutineer can be -in principle- ported to the e-balloting setting.

Q12 What costs are associated with the technological options around e-balloting and also non-technological mitigations?

An e-balloting system can be designed so that it utilizes standard computing equipment, such as tablets, smart phones or desktop computers. While the cost of such devices can be substantial, in many cases, they are already in the possession of the election participants. Furthermore, it is also possible to retain some of the potential benefits of e-balloting by using a hybrid approach between e-voting and postal voting, where, say, paper ballots are distributed by post containing personalised vote-codes that can then be submitted via very lightweight devices (even a regular telephone). In this case, the client-side costs become minimal. In such circumstances the cost of e-balloting can be expected to be even lower than postal voting at least in an amortised sense. This is because depending on the system, the server side will be an important (but one time) upfront cost that needs to be quantified.

Aggelos Kiayias
Chair in Cyber Security & Privacy
University of Edinburgh

For and on behalf of UKCRC

Acknowledgements. A number of UKCRC members as well as e-voting researchers outside UKCRC provided input, suggestions, comments and corrections in earlier drafts of this document and are gratefully acknowledged here. These are:
Ann Blandford (UCL), Michael Fourman (University of Edinburgh), Feng Hao (Newcastle University), Mark Ryan (University of Birmingham), Steve Schneider (University of Surrey), Thomas Zacharias (University of Edinburgh), Bingsheng Zhang (Lancaster University).

Verifiable Elections without Random Oracles. ACM Conference on Computer and Communications Security 2015: pp. 352-363 and Chondros et al. D-DEMOS: A Distributed, End-to-End Verifiable, Internet Voting System. ICDCS 2016, pp. 711-720.

[22] See e.g., the DEMOS system cited above.