

CESG report on eVoting Security - Response of the Centre for Computing and Social Responsibility, De Montfort University

Dr. N Ben Fairweather
Research Fellow

This is a response to the 2002 CESG report entitled “e-Voting Security Study”
(<http://www.edemocracy.gov.uk/library/papers/study.pdf>)

Annex A

We are deeply concerned by the *key principle* (para 59), since we do not believe it can ever be possible for a voter to “receive assurance that their vote was recorded as it was intended” in an unsupervised location without opening the way to coercion and vote-buying.

At Paragraph 61 we are asked “In an e-democracy system what would be an acceptable level of misuse?” The perception that every vote counts, and that the result can be decided by those votes is an important element in encouraging people to vote. If security problems or misuse significantly undermine this perception, our democracy is in severe trouble. In our opinion misuse must be kept at sufficiently low levels that it can be proven both to not have affected who is declared elected in each division, and that the percentage share of the vote for each candidate (or party in list elections, such as European elections), can be shown to be in error by no more than 1% (since relative results at previous elections have a substantial effect on the electoral chances of candidates at future elections). Beyond this, even if these criteria are met, the proportion of voters who complain that they were prevented from voting by technical considerations

when they were seriously intent on voting must not be allowed to rise above the levels experienced with traditional ballot boxes and postal voting (on the pre-2000 rules).

From a brief examination the security profile in Annex A, we are provisionally willing to endorse Recommendation 1 at paragraph 63, in respect of pilots, but with a number of reservations as outlined below, and noting that it appears that it would be appropriate for any system to meet BS7799, which is not mentioned. This security profile appears more realistic than those that appear to have been implicit in the 2002 electronic voting pilots.

Annex A: 3.1.1

While internal attackers are in principle susceptible to punishment, this requires both that security breaches are traced to them, and that there is an inclination to punish them. If internal attacks successfully change the result of a General Election, those taking power may not be inclined to allow the punishment of those that have brought them to power. At a less dramatic level, there may be a temptation on those responsible for a system that has suffered a security breach to cover-up the breach.

Given the extent of the damage insiders could cause, and the incentives that they may have to do so, the security against such attacks must be very high, with good detection and response mechanisms built in any voting system. Even if there are no successful insider attacks, the suspicion that they might have taken place could fatally undermine confidence in the electoral system. For an electronic General Election security must be sufficiently good to ensure that such a suspicion is not widespread.

Annex A: 3.2.2

We are deeply concerned that there is complacency about vote buying and coercion. We understand that in the pilot held in Swindon in May 2002, party workers called on voters and offered them a chance to vote using the party workers' mobile telephone. While we have no reason to believe that coercion took place, the opportunity clearly arose. While there might not be large scale organisation, it seems quite plausible to us that significant numbers of party workers will overstep the mark into illegality in closely contested elections. This is especially worrying since some non-mainstream parties, such as the British National Party, may intentionally resort to illegal means to influence the election.

Annex A: A4.1

The eleven principles identified appear appropriate, and, depending on correct interpretation, could be complete as a set of security principles for electronic voting. However, it is important that they are not met in ways that are incompatible with other key principles that should underlie any electronic voting implementation: the two other key principles are simplicity of the voting process and equity of access. We are deeply concerned that these principles have not received sufficient attention in the CESG “e-Voting Security Study”, resulting in proposals that meet very many of the security considerations vastly better than any commercially available evoting solution, but which are unworkable.

Annex A: A4.2 OS3 and A.5.3.1 OS3

We are concerned that technical means that allow votes to be attributed to voters in relation to the determination of electoral fraud will mean that the long term secrecy of an individual’s vote cannot be assured, since computerised sorting of votes would be possible. The fear is that if the political climate were to change, a regime may be able to use such methods to identify those who have voted for its opponents vastly more easily than would be possible with paper ballots, and assurance that the ballot has been destroyed is vastly more difficult to achieve if it is computerised than if it is marked on paper. Given the rarity with which courts require the attribution of votes to individuals, and the miniscule number of votes affected, we are doubtful that making technical provision for such attribution is worth the risk, given the number of formerly democratic regimes that have fallen under totalitarian control at one time or another (including Germany, France, the Netherlands, etc).

Annex A A5.4.2

While the requirement is correct in relation to direct evidence of how the vote is cast, the same problem arises with indirect evidence that can be interpreted in conjunction with other material that a coercer or vote buyer can obtain from the voter, or possibly from the waste stream.

Annex A A5.5.3

We have no doubt that for a General Election or another election or referendum of high importance; a system of security involving tokens is essential.

Annex A A5.8.1

The requirement for strong communications integrity measures is entirely appropriate. We are, however, concerned that elsewhere in the study mention is made of practical use of methods, such as SMS, which cannot support this in any meaningful way. Methods that cannot support sufficient communications integrity measures should be explicitly rejected.

Annex A A5.12

In our opinion strong 'vetting' is essential, and we are relieved to see it is specified. We note, and are deeply concerned, that no mention is made of the additional problems that may arise if operators are not physically located in the United Kingdom. Since eVoting pilots have already made use of operators located offshore, this is a live concern. We would recommend that the system is physically located in the UK in its entirety so that vetting can be conducted by UK authorities, and staff are unambiguously subject to UK law. We would also recommend that no staff are permitted to work on the project who have criminal records or have been subject to criminal investigation related to fraud, theft, corruption, falsification of documents, computer-related crime and the like, in addition to political subversion. Where it is impossible to ascertain whether an individual has been subject to such investigation or punishment, because they have been abroad for a significant period, they should be prevented from holding trusted positions in the election system.

We also recommend the use of two person rules in addition to vetting for key positions.

Annex A A 5.14

We are concerned by the talk of EAL4, since we believe, with Mercuri (2001, p148) that covert channel and higher attack resistance analysis are needed. We are even more concerned about talk of relaxation of requirements under Fast Track Assessment.

We would anticipate any reasonably secure electronic voting system to make use of both open source and contracted independent scrutiny techniques in addition to formal evaluation.

Recommendations 2-7 and Annex C

We wholeheartedly endorse the conclusion that “e-voting in a General Election would be a significant and attractive target” for attackers (paragraph 64).

While we think that it is desirable for electronic voting systems to meet *Recommendation 2 (paragraph 65)*, we are concerned that attempting to meet such a recommendation will prevent systems from meeting other, more important, criteria, such as at least one of simplicity of voting or secrecy and security of the vote in transit.

While *Recommendation 3* is desirable, it woefully fails to capture the true essence of usability requirements (as does paragraph 66). Having a consistent voting system, the operation of which is consistently beyond the capabilities of a significant proportion of the electorate, is worse than having different techniques for different client devices. Focus group research conducted for the Government (BMRB 2002) has clearly indicated that inputting the twenty digit sequences that are necessarily required for security is considered “‘*unacceptable*’ by both younger and older respondents.” Simpler methods of input are essential for a large proportion of the electorate, and considerations of equality suggest that interfaces should enable unassisted secret voting even for voters with learning difficulties.

We wholeheartedly support the use of out-of-band transmission of secret information to the voter (paragraph 67), however, we do not believe that it is possible to meet *Recommendation 4*, and employ a “mechanism ... to negate the requirement for the delivery channel infrastructure to provide confidentiality and the integrity of the vote” while meeting other more important requirements, such as both simplicity of voting and the secrecy and security of the votes in transit.

We concur with *Recommendation 5 (paragraph 68)*, that “Measures need to be taken with both the infrastructure providers and any e-voting service providers to ensure an acceptable level acceptable of availability of e-voting systems”, and consider this to be a very challenging recommendation. We suspect that higher effective levels of availability can be obtained if systems can automatically switch between networks (for example from direct dial-in using the Public Switched Telephone Network to using the internet and vice-versa).

While scratch-card like solutions (paragraph 69) as outlined in Annex C do very well at meeting security considerations that previous pilots have fallen woefully short of, and piloting them may be worthwhile (*Recommendation 6*), the failure of the system outlined to prevent vote buying and coercion makes it unsuitable for use outside pilots. We strongly suspect that any pilots will amply illustrate the usability problems of such an approach, and as such look forward to their conclusions. We have further concerns with the proposal in Annex C, as outlined below. Given this, we believe it is pointless to “consider how to extend the concepts and mechanisms proposed in Annex C to electoral systems other than first past the post.” (*Recommendation 7*).

Annex C: C1

We are deeply concerned by the proposal (at paragraph 232) that “a smaller-than-usual number of physical polling stations would be provided for the election”. No matter how simple an electronic voting technique is devised, a significant proportion of voters will wish to use traditional polling stations for the foreseeable future, since a significant proportion of the electorate is technology-averse (these will be disproportionately elderly voters). If a smaller-than-usual number of physical polling stations is provided, the distances such voters will have to travel to get to these polling stations will be increased, and this can be expected to have an adverse effect on turnout, especially since elderly voters are disproportionately likely to vote at present, and are also disproportionately likely to have mobility difficulties. Even if it does not affect turnout, any such reduction in the number of polling stations will constitute discrimination against voters with disabilities who are unable to use the electronic voting techniques and against voters who are technology-averse.

Annex C: C4

It appears to us that the threats of vote modification and deletion in transit mentioned at paragraph 255 are significant even with the techniques proposed in Annex C. Alteration without knowledge of content is unlikely to result in valid votes for some other

candidate, but could still be an effective strategy to affect the result of an election, since there are clear geographical correlations with voting: altering a significant proportion of the votes that came from a Labour voting area, could, for example, prevent the election of a Labour candidate who rightfully would be elected. While with response IDs correctly used by voters, voters would have an opportunity to overcome such modification, there must be a suspicion that a significant proportion of voters would fail to check responses and others would give up if a number of attempts to vote all failed. It is thus vitally important that unusually high levels of incorrect voter identity/candidate strings are detected and investigated. The baseline data against which to make such judgements could, and should, be collected in pilots, and the collection of such baseline data is perhaps one of the most useful functions of pilots.

While the use of personalised response IDs enables individual voters, if sufficiently educated, committed and thorough, to ensure that their vote has been received, it also opens the way to confidence attacks, whereby response IDs are changed in transit, thus giving large numbers of voters the impression that their vote has not been correctly cast. This could, in turn lead to large numbers of repeated attempts to vote, and effectively amount to an indirect denial of service attack. There are particular opportunities for this attack, since the transmission of response codes may well be easier to for attackers to detect than the transmission of votes, and since it is with data flowing away from the election system, it may be even more difficult for the authorities to detect such an attack directly than it would be with modification of data flowing to the election system.

Recommendations 8-15 and Annex B

We are aware of the security concerns with a change of voting paradigm (paragraph 70), and suspect they will occur in much the same way with any eventual evoting solution. We thus support and welcome *Recommendation 8*, and note that such a study is also essential given the introduction of postal voting on demand by the Political Parties, Elections and Referendums Act 2000.

We welcome *Recommendation 9* (paragraph 71). We hope that any study will meet the considerations mentioned above in our discussion of Annex A A 5.14.

The possibility of multiple voting (paragraphs 73-75) is worrying to us. While there is nothing in principle wrong with an arrangement where voters are permitted to cast as many votes as they like and all but the first vote are discarded, we strongly suspect that such a system will be sufficiently at variance from public expectations as to make it unacceptable. It might be possible for a massive programme of public education to

overcome this difficulty, but it will have to work against knowledge of other internet and telephone voting systems which permit multiple votes to be counted. We are convinced that the only rule of precedence that will not increase the risks of vote buying and coercion is to accept the first vote received in all circumstances, but allow for the possibility of tendered votes from a supervised polling station as at present. This is because, as illustrated in paragraph 76, a voter subject to coercion may succumb to such coercion between when they have cast the vote for their choice of candidate and the end of the election, and it is easier for the coercer to prevent the voter from subsequently changing their vote between when it was cast as required than it is for a coercer to prevent a voter both from voting before they are coerced and from requesting a tendered paper. It is vitally important as part of such a system that voters are able to discover whether a vote has already been cast in their name, so that they can request a tendered paper if required. While it is appropriate for the Government and the Electoral Commission to consider the rules of precedence (*Recommendation 11*), the conclusion they should draw is obvious. We welcome *Recommendation 12*, that “The Government should ensure that the issues associated with coercion ... are studied”, but are most anxious that such studies are not restricted to issues also associated with multiple voting.

Vote selling and coercion as a result of the transmission of vote confirmations is a deep problem. We welcome *Recommendation 13*, that “The government should ensure that the use of vote acknowledgements and the risks of vote selling/vote fraud are studied.”, and would urge that any system that cannot keep levels of vote selling, vote fraud and coercion to levels as low as have been achieved in recent decades in England, Wales and Scotland be rejected on those grounds.

The *Recommendation (14)* that “Any future trials should assess how e-voting services can be delivered on a larger scale” is welcome. However, we are concerned that any regionalisation of services should keep them sufficiently local as to enable local knowledge to be brought to bear, and that no more than 10 Parliamentary constituencies are covered by a single regionalised service, so as to minimise the effects of any successful attack on the service.

This consultation is a welcome opportunity for “the public, academic community, and commercial suppliers” to indicate whether proposals could command broad public support, which will be vital (*Recommendation 15*), and we welcome the recognition that such independent scrutiny is essential. We are, however, concerned that no proactive attempt has been made to collect the opinions of the academic community, when the identity of most of the key players is clearly known: relying on members of that community chancing upon websites and links within those websites is inadequate. We are confident that the Government would not take a course so risky as the full-scale implementation of eVoting without proactively collecting the opinions of the academic electronic voting community.

Annex B: B8.6

Paragraph 213: We do not accept that a paper audit trail requires the identity of the voter to be marked on the paper versions of the votes, and have seen no evidence of any academic recommending such a proposal. This appears to us to be a misinterpretation of the work of Mercuri and/or Chaum. The only reason to mark paper versions with the identity of the voter would be to replicate the current UK-specific possibility of identity being linked to a vote under a court order, which we have not seen any academic commentator on the technical aspects of electronic voting recommend. If this was not required, the most data that would need to be associated with a vote could only implicitly identify the voter, and we recommend that care is taken in the design of the audit to avoid even having data that could implicitly identify voters stored with the voter's choice of candidate.

References

Mercuri, Rebecca (2001) *Electronic Vote Tabulation: Checks and Balances* PhD thesis, University of Pennsylvania

BMRB International (2002) *Public Attitudes Towards the Implementation of Electronic Voting Qualitative Research Report* online at (<http://www.local-regions.odpm.gov.uk/egov/e-voting/03/05.htm#4>), accessed 31.10.2002.