Voting Technologies and Trust

Article *in* IEEE Security and Privacy Magazine · September 2006

DOI: 10.1109/MSP.2006.140 · Source: DBLP

2 authors:

Brian Randell
Newcastle University
229 PUBLICATIONS **14,178** CITATIONS

SEE PROFILE

Peter Y. A. Ryan
University of Luxembourg
263 PUBLICATIONS **5,111** CITATIONS

SEE PROFILE

Voting Technologies and Trust

Brian Randell

Peter Y A Ryan

School of Computing Science

University of Newcastle upon Tyne

[{brian.randell, peter.ryan}@ncl.ac.uk]

26 May 2005

Abstract

In this paper, as a step towards the ultimate aim of developing an e-voting system that would be likely to gain and retain the trust of the general voting public, we describe a design for a manual voting scheme that has, we claim, significant security-related advantages over existing well-trusted manual schemes. We then use this design as the basis for a small set of (in most cases partially-automated) voting systems which could improve the efficiency of our proposed manual voting scheme, without endangering the public's trust. Our approach to the design of these schemes is thus as much socio-technical as technical.

Keywords: e-voting, security, insubvertibility, trust, trustworthiness

1. Introduction

Our goal is to develop an e-voting scheme that is both secure and sufficiently understandable to gain as high a level of public trust as is achieved by a number of existing manual voting schemes, such as that in current use in the UK. Such a scheme would, we suggest, need to be regarded by the general public as being as understandable and at least as trustworthy (*i.e.* dependable and secure) as the system they are already used to.

Note that trustworthiness is a necessary, but by no means always sufficient condition for achieving trusted status. The challenge we have chosen to address is therefore as much a socio-technical as a technical one – hence differences between the voting practices in different countries are highly relevant. We gear much of our discussion to the present UK system, though in later sections of the paper we do attempt to generalise our discussion somewhat.

The problems of ensuring public trust in the results of elections have been a matter of concern since the time of the ancient Greeks who, in connection with various legal, commercial and government activities including elections and lotteries, preferred to put their trust in simple gadgets and devices, rather than just in potentially-devious officials [Brumbaugh 1996]. In particular, their senate elections were carried out not by a simple showing of hands but by issuing little clay balls to the senators, who cast their votes by dropping these in the appropriate pot. Paper ballots were first used by the Romans, and the use of standard voting forms bearing the pre-printed names of the candidates was introduced in Australia almost a hundred and fifty years ago.

The earliest voting machines date back just over a hundred years, and various types of voting machines and vote-counting machines have been used extensively, particularly in countries such as the USA which tend to have relatively complex voting requirements. (A very accessible history of voting systems and machines is given in [Jones 2003].)

The present-day voting process used in the UK national elections [Electoral Commission 2005] is a manual one, not dissimilar to the original Australian scheme, which involves the use of paper ballots with a column of candidates' names printed down the left-hand column, and a right-hand column which provides a corresponding set of boxes in which a vote or votes can be marked – see Figure 1.

Figure 1: A conventional ballot paper

The entire manual voting process takes place under the close supervision of a set of independent officials, and also of representatives of the rival candidates, under the protection of a strict legal regime. It involves (i) attendance at a voting station ("polling place") at which the voter identifies herself and is given a ballot paper, marks her vote on this ballot within the privacy of a voting booth, and posts the completed ballot through a slit in a locked, sealed box, and (ii) the secure transport of these boxes from the voting stations to a vote counting centre, where the boxes are unlocked and unsealed, and the manual counting of the votes takes place.

Voters must previously have ensured that their names are on the electoral register. They have to cast their votes at a particular voting station, and each such station has a list of the voters, extracted from the electoral register, who are registered to vote there. This list is marked as each voter is given a ballot paper. Thus the same individual attempting to vote more than once or different individuals trying to vote using the same identity, especially at the same voting station, are fairly readily detected. (Potentially invalid votes, of various types, are identified at the vote counting station, and put to one side while the vote counting proceeds. Detailed consideration of such votes is undertaken only if their number is great enough that the result of the election could be affected, something that can be determined at constituency level in the case of UK General Elections.)

The close supervision of vote casting and vote counting, the fact that the system is based on physical evidence that is retained under seal and can be re-examined if necessary, plus the simplicity of each of the stages of the voting process, and indeed of the process as a whole, are we suggest what causes it to be regarded by all concerned as trustworthy, at least with regard to its ability to deliver an adequately accurate result, albeit sometimes only after repeated recounts in the case of close electoral races. It has given rise to very little controversy, compared to that which has arisen in recent years around the use of various semi-automated or automated systems, especially in the USA [Jones 2004a]. However it

benefits from the relative simplicity of UK elections, which in most cases involve choosing just one candidate from a short list of candidates.

There is one concern that is sometimes voiced regarding the confidentiality of each vote. Present practice in the UK involves the ballot papers carrying an inconspicuous identification number, as portrayed in Figure 1, (actually it is printed on the reverse side of the paper), aimed at preventing the use of counterfeit ballot papers, and to assist with the detection of alleged fraud. Ballots are torn out of a book of numbered ballot papers and their similarly-numbered counterfoils, in sequence, and stamped with an identification of the voting station, by a supervised voting station official. The voter number, as given in the electoral register, is recorded on the counterfoil when the voter is given her ballot paper in the voting station.

This procedure, the public are informed, is solely to assist any enquiry that might be called for after the election should there be allegations of impropriety such as vote rigging or multiple voting. Assurances are given that its purpose is not to determine individual votes – and these appear, at present, to be generally accepted. (This is perhaps in part because the task of tracing back from a large set of ballot papers to the relevant voting stations' counterfoils in order to check some particular aspect of the voting process is evidently a non-trivial manual task, in fact one that has apparently – despite rumours to the contrary – not been deemed necessary in any UK parliamentary election since 1911 [Electoral Commission 2003].)

2. Trust – how it is gained and lost

> "We place and refuse trust not because we have torrents of information (more is not always better), but because we can trace specific bits of information and specific undertakings to particular sources on whose veracity and reliability we can run some checks." [O'Neill 2002]

Trust is usually gained incrementally, and can be lost abruptly. The existing UK manual system has been in use for many years, and with the exception of the issue of the confidentiality of individual's votes, receives little criticism. Currently there is however a general concern about the level of voter turnout, which compares unfavourably with that in a number of other Western European countries. This is motivating official trials of alternative schemes and plans to investigate further ones, such as telephone and internet voting, in the hope that one or more will prove more convenient than the present manual process and hence encourage more people to vote. One such trial, which has been used in several locations in recent UK local elections, has been the replacement of the use of voting stations to which voters had to go in order to cast their votes by postal voting – it is noteworthy that though postal voting is claimed to have increased the number of votes cast, it has also given rise to a significant number of allegations of voter fraud, and indeed some successful prosecutions [BBC 2005]. Indeed, it could be argued that, in part at least, the increased turnout is due to fraudulent voting.

It is our view that the current level of trust in the manual system used in UK national elections is due both to its many years of unchallenged use, and the fact that the general public can readily understand the system and believe that it has the characteristic that a large number of votes cannot be subverted (changed, replicated or lost) other than by the malicious activities of a large number of individuals, who would have to act for the most part in collusion. In fact we would argue that the most useful and generally understandable measure of the merit of any voting system is what we will term its **insubvertibility**,[1] a robustness-related characteristic that we suggest be assessed by dividing the number of votes that could be

[1] The OED contains a definition for *insubvertible* ("incapable of being subverted") – the term *insubvertibility*, ("the quality of being insubvertible"), though not actually in the OED, seems rather appropriate for our needs.

altered, faked or lost into the number of people who are needed to achieve such alteration, faking or loss. (A more detailed approach to measuring the actual robustness of a system against security threats is proposed in [Littlewood 1994].)

The notion of insubvertibility relates directly to the question of how much trust the voter is expected to place in how few people, and to the transparency of the voting process. (For simplicity our suggested method of estimating insubvertibility does not distinguish between the different types of people who might have to be trusted – officials, political representatives, and technical experts – leave alone encompass such difficult to assess factors as likelihood of collusion, difficulty of exploitation, risk of detection, etc.)

In what follows we will take insubvertibility and understandability as the crucial characteristics that need to be maximised. Both can, unfortunately, very easily be badly affected by ill-thought-out schemes of electronic voting, in which a very small number of people in the right position might well be able to subvert the entire election! Other important characteristics are of course usability, efficiency and availability, *e.g.* in the face of denial-of-service attacks[2]. (We regard the issue of ballot secrecy (both voter privacy and resistance to vote selling and coercion) as being just one aspect of insubvertibility – and ideas such as voter receipts, encrypted votes, open source voting software, etc., just as possible contributors to achieving it, rather than necessary system requirements to be placed on e-voting.) One can contrast these design aims, in particular that of maximising insubvertibility, with those that evidently guided Diebold, Sequoia, etc., regarding the development and deployment of their touch screen voting devices and systems. Such systems are subvertible in the extreme, as shown by, for example, the Johns Hopkins report [Kohno 2004].

The approach we take is to explore, incrementally, whether and how the existing manual UK voting system could be improved, in particular with regard to vote secrecy, accuracy and overall system efficiency (via the introduction of automation), without compromising the system's insubvertibility, understandability and usability. In effect, we are at least in part being guided by the maxim that "a complex system that works is invariably found to have evolved from a simple system that works" [Gall 1975] (The approach is also reminiscent of the aphorism, usually attributed to either Peter Landin or Edsger Dijkstra, that "it's easier to make a correct program efficient than an efficient program correct".)

Ideally we would like to eliminate the need to trust components of the system, whether they are technical or human, entirely. Schemes such as Fully Auditable Electronic Secret Ballots [Schoenmakers 2000], Secret-Ballot Receipts [Chaum 2004], VoteHere [Adler 2000] or Prêt à Voter [Chaum 2005] in large part achieve this, at least with respect to the accuracy requirements. However with such systems one still must ultimately trust in certain claimed properties of the cryptographic primitives. Moreover, the assurances that can be given regarding such systems are subject to certain probabilistic and computational assumptions. These are both issues that require highly specialised knowledge to appreciate properly.

3. A "Scratch Card" Voting System

In order to improve the voter secrecy provided by existing manual systems as used in the UK we suggest use of a ballot paper based on that used in the Prêt à Voter scheme. In this scheme:

- the ballot papers are perforated vertically so that the column with the list of candidates can readily be separated from that on which the voter has recorded her vote,
- the order in which the candidates are listed varies randomly from ballot paper to ballot paper, and

[2] Problems of availability, even in the face of denial of service attacks, are we believe susceptible to standard solutions rather than specific to voting, and are not further addressed here.

- the voter is allowed to choose a ballot paper for herself at random from a large bundle of such papers.

However, as shown in Figure 2, and in contrast to the Prêt à Voter scheme, at the foot of *each* column is printed a unique vote identification number (VIN). The left-hand column of the ballot paper (LHC) constitutes a vote receipt that can be retained by the voter after she has voted, while the right-hand portion (RHC) is carried forward into the vote counting process. Although the LHC does not, once separated from the RHC, provide any indication of how the voter cast her vote, it does provide an identifiable record of the fact that a vote has been cast, a record that can later be checked against the numbers on, or recorded from, the collected set of RHCs, should this be required.

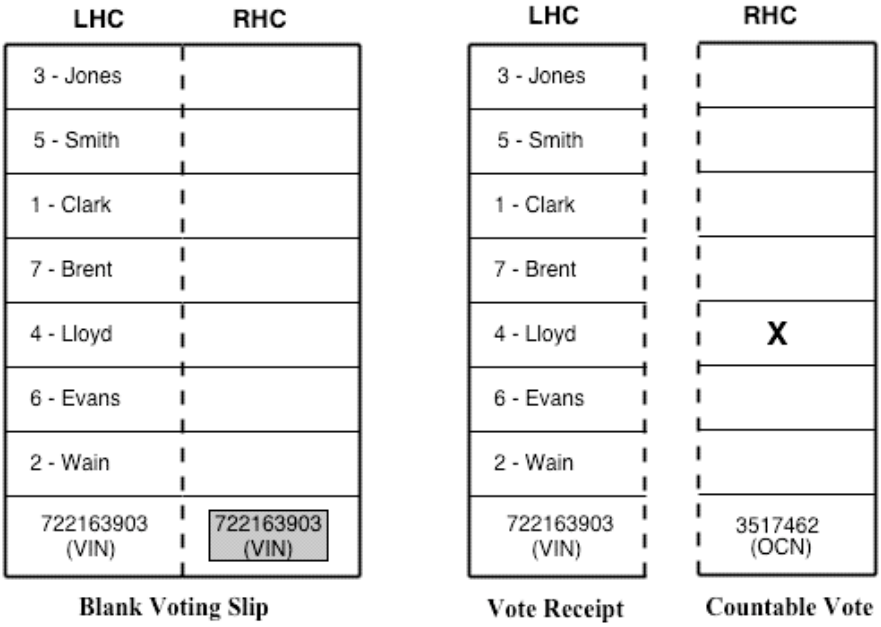

Figure 2: A ballot paper – before voting and after it has been made countable.

The crucial aspect of our scheme, inspired by the cryptographic technique involved in the Prêt à Voter scheme, is that the RHC is, in effect, a so-called "scratch card", in that it contains a small rectangle of opaque coating which is initially obscuring a pre-printed code. This code (OCN) identifies the order in which the candidates' names were printed in the left-hand column. The copy of the VIN at the foot of this RHC is printed *on* this opaque coating. This coating can be scratched off, an act which simultaneously destroys the VIN and reveals the OCN. Up until the moment the VIN is scratched off (and, if any record of it has been kept, this record has also been destroyed) then it is possible to use the VIN as evidence that a vote has been cast, and has not been subsequently lost.

As well as permitting the voter to choose her own ballot paper at random, she would also be permitted – indeed encouraged – to take other ballot papers and (i) to assure herself that they varied with regard to the ordering of the candidates, (ii) to scratch off the VINs (thereby invalidating their use as ballots) and so (iii) verify that in each case the revealed OCN matched the order of the candidates. (By this means she can be reassured that the still-concealed OCN on the RHC that she actually uses in order to cast her vote is in all probability correct, i.e. matches the candidate ordering.) The testing and discarding of RHCs should be done under the supervision of the polling station officials.

The above uses of the term "random" are rather casual – true randomness of the ballot papers is probably most fully ensured by inviting independent auditing authorities to take a random sample of ballot papers before the voting phase starts. They can perform statistical checks on the distribution of candidate ordering, the uniqueness of the VINs and remove the scratch strips to check the revealed OCNs match the candidate ordering in each case. Further random

checks could be performed during and (on left over ballot papers) even after the voting period. This exactly mirrors the procedures of the Prêt à Voter scheme.

Actual vote casting requires the voter to proceed to a booth with a single ballot paper with its VIN strip still intact. In the booth, she indicates her vote by placing a cross in the appropriate cell on the RHC against the candidate of her choice in the usual fashion. She then splits the ballot paper along the perforation down the middle and posts the RHC into a locked ballot box, leaving the scratch strip intact, so as to preserve the secrecy of her vote. She can retain the LHC as her vote receipt.

When the vote casting period has ended, the secure boxes of votes (RHCs) are taken from each voting station to a vote counting centre. Any RHCs with damaged or missing scratch strips that show up in the counting stage should be discounted, though this has to be done under supervision so as to avoid opening up possibilities for vote spoiling.

In order to interpret the vote value encoded on each RHC, the VIN strip must be scratched off to reveal the OCN hidden underneath. The crucial property of this kind of scratch strip is that the process of revealing the hidden information underneath will destroy the information carried on top of the strip.

Before the RHCs have their VINs scratched off, however, the VINs would be recorded and published (e.g. via a secure web bulletin board) so that each voter can use her vote receipt to check that her vote was indeed entered into the counting process. Ideally, such recording of the VINs should occur immediately before they are scratched off, and under close supervision, in order to ensure that the posted list exactly matches the numbers on RHCs entered into the device or process that removes the VIN scratch strips. This will provide a check that no votes have been lost and no fake ballot papers have been injected between the vote casting and the vote counting stage.

The task of scratching the VINs off all the RHCs can be thought of as destroying the link on the RHC to the vote identification number and replacing this by a link from the RHC to the vote value. It is carried out by officials at the vote counting centre, and of course also needs to be supervised so as to ensure that it is carried out completely, and that no attempt is made to undermine the anonymity of the voting by recording VIN-OCN pairings as the one is scratched off to reveal the other. Ideally this process will be done in such a way as to shuffle the RHCs, so as to preclude associating a sequence of OCNs with any recorded sequence of the VINs that had hitherto obscured them. However, even if there is relatively little scrutiny of the act of scratching off the VINs, the overall confidentiality provided by the overall process is in practice likely to be generally regarded as exceeding that of the present-day UK voting process, given that the latter retains a tell-tale number on each ballot paper throughout the voting process, as well as carrying a clear indication of the actual vote. (We are assuming that other aspects of the existing UK scheme, aimed at authenticating voters and preventing multiple voting, would still be employed.)

Once their OCNs have been revealed the RHCs could be used in a near-conventional process of (well-scrutinised) manual vote counting. This process might for example first involve sorting the RHCs into separate piles, according to the different OCNs on them, tallying each pile separately, and then using the codes to determine how these tallies are to be combined into an overall vote count.

Given the general public's experience of and trust in scratch cards (which are likely to be even more familiar to them than ballot papers) and in the act of shuffling playing cards, we believe that this vote counting process and indeed the whole voting scheme could gain a level of acceptance from the public regarding its overall trustworthiness comparable to that enjoyed by the manual scheme that is currently in use in the UK. The additional vote secrecy it provides should also be manifest to the general public. However, the scratch card scheme's advantages over the existing manual scheme are not limited to vote secrecy. The fact that candidates' names are not given in the same order on each ballot paper can be regarded as an

additional benefit, as there is evidence that a fixed candidate order can have an untoward influence on votes.

4. A possible enhancement

In this section we describe two elaborations of the basic, scratch card scheme introduced in Section 3 above. The resulting scheme is rather more robust in several respects, and is a closer analogy to the Prêt à Voter scheme.

This scheme again uses the two strip ballot papers as before except that now we omit the VIN number on the LHC. The voter makes her mark, feeds the ballot paper into a device that detaches and destroys the LHC and scans the RHC. It produces two photocopies of the RHC, one is returned as her receipt, whilst the other is posted into a locked and sealed audit box (perhaps after being viewed under glass and confirmed by the voter in the manner of the "Mercuri method" [Mercuri 2002]). The "real" RHC (with scratch strip still intact) is posted into the locked and sealed ballot box.

The ballot boxes are shipped off to the vote counting centre as before but now the VIN numbers and positions of the "X" marks are published. As before, voters can check these, but also auditors can do random checks of the correspondence between published receipts and the paper audit trails stored in the audit boxes. Note that, as with Prêt à Voter, the receipts do not reveal that way the vote was cast.

This scheme has a number of advantages over the scheme presented in Section 3:

- Receipts do now reflect, in encrypted form, the voter's choice and it can be checked that the "X" has not been altered in transit.
- The checks on the list of published VIN numbers and positions of the "X" performed by the voters are supplemented by the auditor checks.
- The approach suggested here has similarities to the Voter Verifiable Paper Audit Trail (VVPAT [Mercuri 2002]) that has been advocated by various experts in the US.

5. From Paper to Mechanism

The question we now address is whether the basic scratch card scheme's various characteristics, in particular those of insubvertibility and understandability, can be retained when various aspects of the scheme are automated in order to speed up the vote casting process and to reduce its costs. We deal with issues concerning vote casting and vote counting separately, and first of all concentrate on systems that retain the use of paper ballots since, in a nation such as the UK where paper ballot are the currently-trusted norm, we believe that it will be much easier to retain public trust if the usage of such paper ballots is retained in some form.

5.1 Retaining Paper Ballots

Particularly where voting is complicated (due to the number of candidates and the number of choices that a voter has to make), there would be merit in the use of a voting machine in connection with the paper ballots. At its simplest, such a machine would be one that could receive a pre-printed ballot paper, check that it is unmarked and still had an intact VIN scratch strip on it, and merely assist the voter with the task of marking this ballot paper in accordance with whatever electoral rules apply to the voting, for example by ensuring that the resulting ballot paper is "guaranteed" to be both legible and valid. This might speed up the voting casting process, and should reduce the number of accidentally spoilt ballot papers. In the US context, for example, the machine might warn the voter of possible under-voting or over-voting.

A more complex machine would also do the actual printing of the ballot paper, after enabling the voter to randomize the ordering of the candidates, for example using a facility that deliberately mimics the action of a mechanical or electronic one-arm bandit, and which then allows the voter to indicate her vote. (There would of course be a need to undertake adequate checking of the design of such machines and their operation, tasks that would be aided by the machines' relative physical simplicity.)

The resulting printed ballot paper then can either have its VIN scratched off by the voter (for purposes of checking that the machine does generate OCNs which match the candidate ordering) so invalidating the ballot paper, or can be used by her to cast a vote as before. The advantage of such a device is that it would presumably give the voters a greater confidence in the randomness of the OCN lists so generated. Whether such confidence is well placed is of course another matter. (The problem of validating sources of randomness, such as gaming machines, is itself the source of delicate challenges.)

Note that any malfunctioning or corruption of the device, at least from the accuracy point of view, would be detectable and verifiable. Thus if the device attempted to print OCNs on the ballot forms that did not match the candidate ordering, should voters check the forms they can demonstrate to an official that the machine is malfunctioning or corrupt.

The fact that such voting machines produce checkable printed ballot papers (of the form shown in Figure 2) should, we argue, ensure voters' willingness to trust that the system is not adversely affected by the use of such machines, even if the average voter has no idea how the machines actually work. (A general public that is already familiar with and prepared to trust existing electro-mechanical voting machines, such as in the USA, would we presume be quite willing to invest at least as much trust, with respect to both accuracy and confidentiality, in a voting process based on the use of such machines as they do in the use of existing voting machines.)

The counting of paper votes (RHCs) could be done using one or more special-purpose devices whose design (possibly, indeed preferably, electromechanical rather than electronic) was so simple and operation so visible that it could be reasonably readily scrutinised and audited. In particular, sorting physical votes into piles and tallying these piles could be done by machines not unlike conventional (albeit old-fashioned) electro-mechanical Hollerith/IBM mark-sensed card sorters – to the front end of which had been added a set of brushes that first removed the coating on which the VINs were printed. (Alternatively, one can envisage use of a machine that processed a large set of votes en masse, removing this coating, before any counting is done.) This type of electromechanical machine is not too dissimilar to the sorts of vote counting machines that have been used and generally accepted (when properly monitored by trustworthy officials) in some parts of the USA for many years.

5.2 Electronic Vote Counting

Major trust concerns arise when one moves away from the use of paper ballots either partly (in that paper voting receipts might still be retained) or completely, so that the vote casting as well as counting is all done essentially invisibly, *e.g.* electronically. Even if the public have good reason to believe that electronic versions of their votes are reaching the vote counting process safely, the problem is to provide the public with continued reason to trust a vote counting process that is not directly visible to ordinary officials and scrutineers.

For simplicity, in what follows we ignore the possibility of any part of the vote counting being done at voting stations, and instead assume that either (i) votes are transported securely in paper form to the vote counting centre, where the VINs are recorded and scratched off and the OCNs revealed, as described in Section 3 above, and the information on the RHC then read electronically, or (ii) the VINs are recorded and scratched off at each voting centre, under appropriate scrutiny of course, and the indication of the candidate choice, plus the OCN that was revealed by scratching off the VIN, are fed into a reader to be securely transmitted electronically to the vote counting centre. Evidently, in the first case it is possible to provide

the voter with a more plausible means of confirming that her vote actually reached the vote counting centre safely.

The votes can then be tabulated electronically, taking into account each vote's OCN, possibly after having first been sorted into separate sets according to the OCN, in much the same way that this process could have been carried out manually with paper ballots. However, vote counting machines, or indeed voting machines, i.e. DRE (direct recording electronic) devices, that have a conventional general-purpose computer and operating system incorporated into them are problematic and likely to remain controversial. Their use normally requires a degree of trust that the more technically-aware voters in particular are likely to be reluctant to provide, given that computers and their software pose major problems to scrutineers and auditors, and the present – very understandable – public concern about software bugs, Trojan horses, viruses, etc. [Lauer 2004].

Indeed, with electronic votes various forms of "online" manual checking by multiple observers will normally have to be replaced or supplemented by (i) prior checking of the design of possibly very sophisticated algorithms and devices, and (ii) ensuring the continued relevance of the results of these checks up to and during the actual voting process. There is for example little point in formally verifying the design of some software employed within an electronic voting system if one cannot be certain that the software has not been subsequently replaced or interfered with – an example of the TOCTOU (Time-Of-Check-to-Time-Of-Use) problem, one which was demonstrated to have occurred quite flagrantly with Diebold's Global Election Systems DRE machines [Harris 2003]. Ideally, therefore, these algorithms and devices should be as simple and as evidently independent of each other as possible, and susceptible to having their operation completely checked via examination of just their inputs and outputs. The use of multiple physically-separate simple special purpose devices would in fact facilitate constructing a case for their combined trustworthiness from arguments about their individual trustworthiness, *cf.* the approach to security via separability [Rushby 1982].

An alternative approach that has been taken by others to the design of electronic voting systems is to attempt to devise and validate means whereby the complete set of activities making up the process, from vote to count, could (i) be achieved entirely electronically, using some sort of cryptographic equivalent of the scratch card mechanism, and (ii) incorporate some scheme for allowing (at least probabilistic) checks to be made that all the votes are being properly accounted for – this is the approach taken in the Prêt à Voter scheme [Chaum 2005]. Minimally, such checks would routinely be made at various stages during the process, and especially immediately after completion of the vote counting and before the election result was announced, not just when for some reason suspicions are raised. Another, rather different fully-electronic approach is described by Schoenmakers [2000]. This enables secret and auditable voting via the Internet, using cryptographic techniques such as verifiable secret sharing and zero-knowledge protocols, together with multiple independent vote-tallying facilities that provide a form of "distributed trust". However, although with such voting schemes the computers and the software involved need not be trusted, the arguments for the trustworthiness of the overall voting system are subtle and require specialist knowledge in order to be properly appreciated.

A very different approach involves the use of a Voter Verifiable Paper Audit Trail [Mercuri 2002] as an adjunct to an electronic voting casting and counting system. With such an approach, the need is to ensure (i) that the audit trail mechanism, rather than the actual voting system *per se*, is adequately trustworthy, and (ii) that recourse will be had to this audit trail mechanism whenever necessary. This latter issue will involve careful and extensive scrutiny of the audit trail and of the operation of the voting casting and counting, if low error rates or subtle attempts at subversion are to be reliably detected.

There is, however, a fundamental requirement for any e-voting system to be not just *trustworthy*, but also *trusted*. Moreover, it has to be trusted by the average voter (with regard to the act of voting), by the electoral officials and political representatives (with regard to the

whole process of carrying out and scrutinising vote recording, tallying and totalling), and as a whole by the public at large and the media. (Similar points are made in [Jones 2004c].) Acceptance of the deployed system's trustworthiness by reputable technical specialists in e-voting, while necessary, unfortunately may not be sufficient to engender such trust, if neither these specialists nor anyone else is capable of explaining the system and the basis of its claimed trustworthiness in very simple and convincing terms. (Realistic trials can of course help, providing these trials involve very extensive and expert – but unsuccessful – attempts at achieving subversion.) Moreover, such explanations must be sufficiently persuasive to counteract the effects of any apparently justifiable allegations about the trustworthiness of the system made by other individuals or organisations who for whatever reason are opposed to e-voting. This we would suggest is an as-yet unsolved (socio-technical) problem.

6. Summary and Conclusions

In this paper, as a step towards the ultimate aim of an e-voting system that is both *trusted* and *trustworthy*, we have (i) described a design for a manual voting scheme that has we claim significant advantages over existing trusted manual schemes, and then (ii) used this design as the basis for a small set of (in most cases just partially-automated) voting systems which could improve the efficiency of our proposed manual voting scheme. This is going a significant step further than that advocated by [Jones 2004c]:

> "What I believe we must seek is a decomposition of the election problem into technological components where the essential properties of those components are subject [accessible demonstration]. This does not require that the internal workings of the system be entirely revealed, but rather, it places each such component inside a shell of easy-to-audit defenses. Another way of thinking about this is that we are attempting to reduce the size of the trusted base of hardware and software to the point that the trusted base can be entirely disclosed and where the logic of that trusted base is clear to a bright high school student."

Our claim is that at least all the manual or partially-automated systems we have described above stand a good chance of gaining and retaining the degree of trust that is accorded to present-day manual voting systems in the UK. Moreover, they provide an increased level of security, together with some degree of voter verifiability in that voters are able to confirm that a ballot paper bearing their VIN number was entered into the tabulation process. This is in contrast to most existing voting systems in which the voters are not provided with any such checking capability. However, it falls short of the level of assurance provided by cryptographic schemes, such as Chaum's scheme, VoteHere and Prêt à Voter, in that the voters still need to trust the mechanisms and processes that strip off the scratch strips and shuffle the resulting RHCs to do so in a way that will not corrupt any of the ballots (e.g., lose ballots, inject fake ballots, alter ballots).

We have argued that carefully designed mechanisms along with conventional scrutiny procedures should lead to good levels of assurance. But we note that the cryptographic schemes are able to replace such trust with cryptographic mechanisms that ensure that any non-negligible corruption during this tabulation would, with high probability, be detected. The trouble is that (i) such a cryptographic scheme is not readily explainable to the general public, and (ii) evaluations provided by technical experts may not be enough to persuade the public to put their trust in it.

Our approach to the design of our schemes and its presentation has of necessity been socio-technical as much as technical, in that we have deliberately tried - in pursuit of user acceptance and trust - to retain the familiarity and simplicity of current well-accepted devices and systems. As a result, in most of our proposals we have deliberately sought to retain at least some use of paper, and to avoid, or at least minimize the use of, electronics and

computers. (For a discussion of such matters see, for example, [Economist 2004] and [Jones 2004b, 2004c].) This, we have found ourselves arguing, somewhat to our own initial surprise, is perhaps one of the most practical ways of achieving and retaining the trust and confidence of the general public in any new automated or semi-automated voting scheme. However this claim requires (i) thorough analysis, e.g. by psychologists and sociologists, concerning the relative importance of the many factors that can affect public trust (see for example [Misztal 1996], [O'Neill 2002] and [Ulivieri 2005]) and how these might apply to election systems, and (ii) proper validation, via extensive trials designed and supervised by expert experimental psychologists and sociologists, not just pilot demonstration voting exercises. (One study we are aware of concerning public trust in e-voting was based on a small-scale trial of the TruE-Vote system [Oostveen 2003]. This found that "The more people trust in the security and the better the usability of the system, the less they will doubt about the ability to verify the count of the vote. . . However, a lot of the variables that correlate with the trust in verifiability have nothing to do with the technology itself, but more with the social context in which the new technology is embedded". The study concluded "People should not just have to trust in the integrity of a voting system or the people who designed, developed and implemented it. . . In order to fully understand citizens' willingness to use electronic voting systems we need to look as much into socio-political issues as into technological issues." [Oostveen 2004])

An alternative approach to the goal of designing an widely acceptable e-voting system is to not to start with an existing trusted system but instead with a sophisticated e-voting system that is believed to be technically trustworthy, for example Prêt à Voter, and try to simplify the design and the description, to the point where one could expect the general public to accept it. This approach continues to be pursued and we would hope that the two may converge. To paraphrase the Landin/Dijkstra quote above: "perhaps it's easier to make a correct scheme accessible than an accessible scheme correct".)

We, and others, have argued that the design of e-voting systems must in fact be treated as a socio-technical problem, and indeed one that might with benefit be treated differently in countries with differing existing practices and attitudes. In fact we believe that at least equal weight must be given to socio-technical issues such as (i) system understandability and usability, and (ii) the roles, both positive and negative, likely to be played by the various people and organisations involved in the overall voting process, as is given to any attestations by technical experts as to the trustworthiness of complex e-voting hardware and software.

The goal that we set ourselves in this paper is very challenging: to develop a system that provides high assurance of accuracy and secrecy with minimal trust in the components of the system, whilst being at the same time sufficiently simple to be generally understandable by the electorate at large. It may in fact turn out to be impossible to achieve all of these in a single scheme, in which case it will be necessary to back off certain aspects of these requirements. We might not require such high levels of assurance, or decide that it is acceptable to allow a greater degree of dependence on certain components or processes. Alternatively, one might decide that striving for complete understandability by the electorate is unreasonable and so strive for "sufficient" simplicity and appropriate explanations and metaphors to achieve acceptance and trust. But the justification of any such decisions is again essentially a socio-technical, or at least a political, problem.

7. Acknowledgements

The suggestion that we use, as a means of comparing voting systems, estimates of the number of people who would have to be implicated in any successful attempt at subverting a given number of votes was made to us by Cliff Jones. He and other colleagues have also commented helpfully on earlier drafts of this paper.

8. References

[Adler 2000] J. Adler et al, *Computational Details of the VoteHere Homomorphic Election System*, VoteHere, Bellevue, WA. (2000).
(http://www.votehere.net/ada_compliant/ourtechnology/technicaldocs/hom.pdf)

[BBC 2005] Judge upholds vote-rigging claims. *BBC News* (4 April 2005).
(http://news.bbc.co.uk/1/hi/england/west_midlands/4406575.st)

[Brumbaugh 1966] R.S. Brumbaugh. *Ancient Greek Gadgets,* New York, Crowell, (1966), 152 pp. ISBN: 0837174279.

[Chaum 2004] David Chaum. Secret-Ballot Receipts: True Voter-Verifiable Elections. *IEEE Security and Privacy*, Vol. 2, No. 1, pp.38–47, (Jan/Feb 2004).

[Chaum 2005] David Chaum, Peter Y.A. Ryan and Steve A. Schneider. *A Practical, Voter-verifiable Election Scheme.* Proc. 10th European Symposium on Research in Computer Security - ESORICS (12-14 Sept. 2005), Milan, Italy.
(http://www.cs.ncl.ac.uk/research/pubs/trs/papers/880.pdf)

[Economist 2004] Electronic voting: The trouble with technology. *The Economist*, Sep 16th 2004.
(http://economist.com/World/na/displayStory.cfm?story_id=3195821)

[Electoral Commission 2003] *Ballot Secrecy*. The Electoral Commission (15 Jan. 2003).
(http://www.electoralcommission.org.uk/templates/search/document.cfm/6127)

[Electoral Commission 2005] *Managing a UK Parliamentary general election - a good practice guidance manual*. The Electoral Commission (2005).
(http://www.electoralcommission.org.uk/about-us/guideukparl.cfm)

[Gall 1975] John Gall. *Systemantics: how systems work and especially how they fail,* New York, Quadrangle/New York Times Book Co., (1975), 111 pp. ISBN: 0812906748.

[Harris 2003] Bev Harris. *Georgia: 22,000 Voting Machines Got a Program Fix, Right Before the Election* (13 Feb. 2003). (http://www.scoop.co.nz/stories/HL0302/S00095.htm)

[Jones 2003] Douglas W. Jones. *A Brief Illustrated History of Voting* (2003).
(http://www.cs.uiowa.edu/~jones/voting/pictures/)

[Jones 2004a] Douglas W. Jones. *Voting System Transparency and Security: The need for standard models*. Submitted to the U. S. Election Assistance Commission, Technical Guidelines Development Committee Hearing on Transparency and Security, National Institute of Standards and Technology, Gaithersburg, Maryland (September 20, 2004).
(http://www.cs.uiowa.edu/~jones/voting/nist2004.shtml)

[Jones 2004b] Douglas W. Jones, Auditing Elections, *Communications of the ACM*, 47, 10 (October 2004) pp.46-50. (http://www.cs.uiowa.edu/~jones/voting/cacm2004.shtml)

[Jones 2004c] Douglas Jones. *Minimizing the Trusted Base*. Presentation for A Framework for Understanding Electronic Voting. Computer Science and Telecommunications Board of The National Academies. (December 9, 2004).
(http://www.cs.uiowa.edu/~jones/voting/nas-cstb2004a.shtml)

[Kohno 2004] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach. Analysis of an Electronic Voting System. *IEEE Symposium on Security and Privacy 2004*. IEEE Computer Society Press, (May 2004). (http://avirubin.com/vote.pdf)

[Lauer 2004] Thomas W. Lauer. The Risk of e-Voting. *Electronic Journal of e-Government*, Vol. 2, No. 3, (December 2004). (http://www.ejeg.com/volume-2/volume2-issue3/v2-i3-art4.htm)

[Littlewood 1994] B. Littlewood, et al., Towards operational measures of computer security, *Journal of Computer Security*, 2 (3) pp. 211-229, (1994).

[Mercuri 2002] R. Mercuri, Government: A Better Ballot Box, *IEEE Spectrum 39, 10* (October 2002) pp.46.50.

[Misztal 1996] Barbara Misztal. *Trust in Modern Societies: The Search for the Bases of Social Order*. Cambridge: Polity Press, (1996), 304 pp. ISBN: 0745616348

[O'Neill 2002] Onora O'Neill. *A Question of Trust: The BBC Reith Lectures 2002*, ISBN: 0521529964, (2002), 108 pp. ISBN: 0521529964. (http://www.bbc.co.uk/radio4/reith2002/)

[Oostveen 2003] Anne-Marie Oostveen and Peter van den Besselaar. *E-voting and media effects, an exploratory study*. Conference on New Media, Technology and Everyday Life in Europe, London (23 -26 April 2003).
(http://www.lse.ac.uk/collections/EMTEL/Conference/papers/Oostveen.pdf)

[Oostveen 2004] Anne-Marie Oostveen and Peter van den Besselaar. *Ask No Questions and Be Told no Lies: Security of computer-based voting systems: User's trust and perception*. In U.U. Gattiker (Ed.) EICAR 2004 Conference D-Rom. Copenhagen: EICAR e.V. ISBN 87-987271-6-8.
(http://www.social-informatics.net/EICAR2004.pdf)

[Rushby 1982] John Rushby. *Proof of Separability – a verification technique for a class of security kernels*. In Proc. 5th International Symposium on Programming, Turin, Italy. Vol. 137, *Lecture Notes in Computer Science*, Springer-Verlag, pp. 352-367 (April 1982).

[Schoenmakers 2000] Berry Schoenmakers. Fully Auditable Electronic Secret-Ballot Elections. *Xootic*. (July 2000).
(http://www.eucybervote.org/xootic2000.pdf)

[Ulivieri 2005] Filippo Ulivieri (ed.). *Trust Across Disciplines*. T3 Group, Institute of Cognitive Sciences and Technologies, CNR, Rome, Italy (7 Mar 2005).
(http://www.istc.cnr.it/T3/map/index.html)