How to Improve Security in Electronic Voting?

Abhishek Parakh and Subhash Kak

Department of Electrical and Computer Engineering
Louisiana State University, Baton Rouge, LA 70803

The usage of electronic voting is spreading because of the potential benefits of anonymity, scalability and speed. The American experience in the 2004 and 2006 elections as well as recent DRE based elections in Europe and Asia have raised questions of its reliability. Electronic voting may be compromised in a variety of ways [1]. There is also the question of verifiability in the light of allegations of fraud or machine malfunction that have surfaced from time to time.

Although by electronic voting we mean here the use the Direct Recording Electronic (DRE) machines, it is to be expected that eventually voting will be done on the Web so that the election could be organized at short notice. These issues are thus of a transitional nature, but they are very important nevertheless.

The general consensus in the data security community is that DRE machines must have a voter-verifiable paper audit trail, and software used on these machines must be open to public scrutiny [2]. This is important not only to examine the software and find bugs, which can then be corrected, but also to increase public confidence in the voting process. If the software is public, no one can insinuate that the voting system has unfairness built into the code, although there may still be those who would question if the validated software was actually used in the system.

On a more theoretical level, it has been proposed [3] that verifiable paper receipts be issued to voters. The idea of visual cryptography has been suggested to encrypt the paper receipt so that it does not reveal how the voter cast the ballot but he is be able to verify his vote. The voter, after the elections are over, goes to a bulletin board (which could be the Web) where the other half of his receipt is posted. The drawback here is that the voter may deliberately tamper with the receipt and falsely suggest that the voting was not accurate. This problem of tampering may be dealt with by using hidden codes in the receipt [4], but that would require examination and validation by another supervisory agency.

Electronic voting is a frontier area of research in the general field of security and cryptographic protocols are being developed to meet its requirements that are analogs of the various parts of the traditional paper ballot system. What makes it so challenging are the conflicting requirements of secrecy and verifiability of the system. Estimates of the results to high degree of confidence can be obtained using statistical sampling, but this is unlikely to be acceptable as the primary means of determining the results of the election. But this does provide a means of cross-checking the result of a straight count.

Secrecy and Verifiability

For fundamental reasons, the requirements of absolute secrecy and total verifiability in electronic voting cannot be met simultaneously. Keeping in mind the stakes that are involved (for example, which party gets to form the government in a county) and motivation for fraud, most protocols today favor verifiability over secrecy.

An important issue in electronic voting is the 'recounting problem'. Recent solutions, that require a paper audit trail, address it to a certain extent. In these schemes, the voter is printed a paper record after he has cast his vote. He examines this receipt, verifies his vote and deposits it into a ballot box. This provides verification data in case of discrepancies or in close elections (but not otherwise), assuming, of course, that the paper trail left in the booth has not been tampered with.

It might be useful to construct a new method which combines the receipt taken home by the voter with the paper record left in the booth. In such a scheme, any fraudulent claim by a voter can be falsified by checking this claim against the deposited receipt. However, in this scheme, a voter cannot maintain secrecy of ballot if he wishes to report fraud.

One major virtue of paper ballots is that the results may be verifiable not only by voters but by their representatives as well. This issue is not addressed adequately by the current electronic voting methods. It is worthwhile, therefore, to reconsider the main differences between paper ballots and DRE.

1. **Change in distribution of security:** In paper ballots the security depends on the integrity of the system consisting of a large number of officials associated with the administration of the election. In DREs, on the other hand, security is primarily concentrated within the machine. This dependability on a machine running on obscure software is a matter of concern.

   Although software may be put to test and code be made public to check for security flaws, there is no guarantee that bugs will not be introduced after the software has undergone testing. There is also the danger that the bugs trigger at a specific time only on the Election Day, or once the election has started and a few hundred votes already cast.

2. **All verification must end inside the polling booth:** Receipts brought back home by the voter could be used by an unscrupulous party to compel him to reveal the vote.

3. **Separation of recording part of the machines from the input panel:** The separation of recording and input portions may be necessary to provide flexibility in developing protocols for verification and recounting.

4. **Electronic recounting procedure needs to be introduced**: This requirement can only be fulfilled by having recording done simultaneously by multiple machines running different software written by different companies. This is to deal with bugs in the software, since it is highly unlikely that two different companies writing DRE software having common input portal would have placed identical bugs in them.

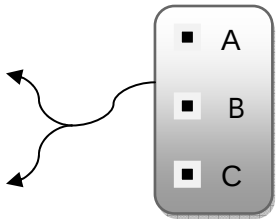
Verification by Permutation of votes

It may be possible to use supervisory (or, redundant) machines if one of the machines is fed "permuted votes".

For example, if 3 parties, say A, B and C are contesting, then the permutation device (permuter) will assign votes of party A to C, B to A and C to B (or A to B, B to C and C to A or any other permutation). Let us assume that the permutation chosen is:

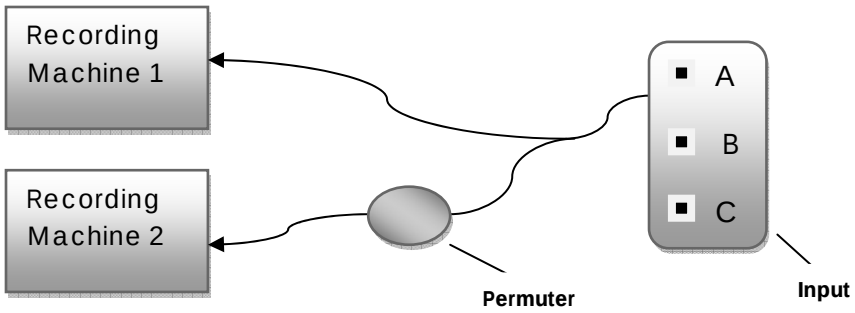
A ⟶ C (i.e. A's votes are assigned to C)
B ⟶ A ….
C ⟶ B ….

We may view the input panel as a key pad or a touch screen machine, which in our case is shown below:



Input panel: representing two parties A and B

If the output is standardized, and the recording machine is not able to distinguish between "genuine" votes and permuted votes. The complete setup is shown below:



Parallel recording: Machine 1 records direct vote and Machine 2 does permuted vote

This scheme would provide a cross-check of election results in the following manner:

Suppose, the genuine votes were supposed to be:
A = 10, B = 8 and C = 10 (Recording Machine 1).

Then permuted votes should be:
A = 8, B = 10 and C = 10 (Recording Machine 2).

Now, if the recording machine is bugged to increase C's votes.

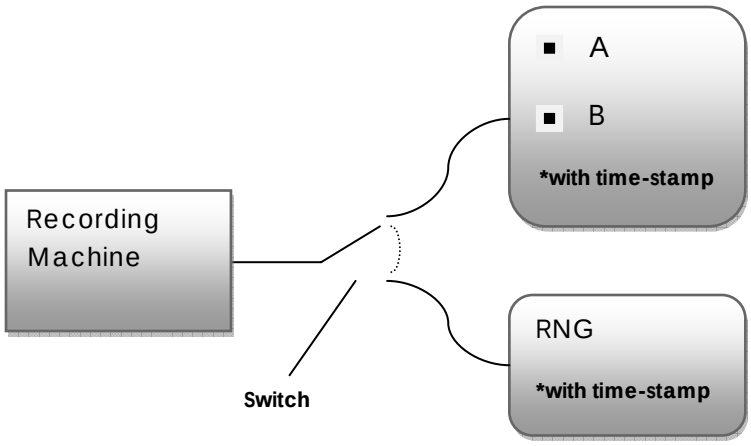
Then Machine 1 will have: A = 9, B = 7 and C = 12.

While Machine 2 will have: A = 7, B = 9 and C = 12.

The permutation is violated when the machine is bugged to favor a party (correct permutations should have been: A = 7, B = 12 and C = 9) and results do not tally as they should. Since the manufacturer would not know in advance which machine will receive a permuted input, there cannot be any preloaded bug in it.

DRE machines with RNG

The security of the voting process may be improved by the use of a random number generator (RNG) to generate votes that are fed into the counting process but subtracted at the end. In a variation, one may add the requirement of time-stamp along with each vote recorded.



Verifying the operation of recording machines using RNG

Once the election process is over, the election officials can verify the votes recorded at those specific time-stamps when RNG was connected to the recording machine.

These schemes will eliminate the need for the voter to bring a receipt home and hence eliminate coercion by political enforcers (common in some developing countries) and maintain secrecy of ballot by achieving a certain degree of distribution of security.

Avoiding coercion using paper receipts

Paper receipts do not provide protection against coercion. The basic flaw in such schemes is that the verification is based on visual reading, i.e. the system provides the voter with a visual proof of his vote in plain text after the election is over. However, this plain text can be read by a third person who might be an enforcer. Hence, in order to make the paper receipts work the verification needs to be "mental". By this, we mean that the system must provide the voter enough proof so as to mentally be satisfied that indeed the vote is recorded as he had intended. However, since he can only mentally verify his vote, he is not able to convince a third person about how he voted.

Formally, we can represent the system as follows:

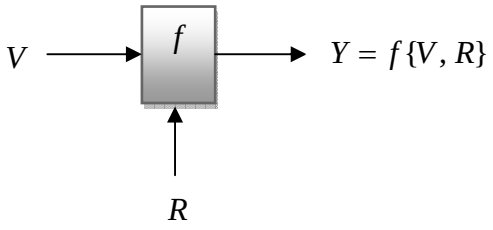
If,

V denotes the vote. It may be the party name, identification number of a party, etc.

R is a random input chosen by the voter at the time of casting a vote.

f is a one-to-one and onto function which is easily verifiable and invertible.

Y is a function of V and R.

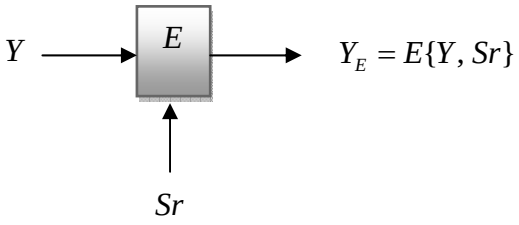


And,

E is an encryption transformation.

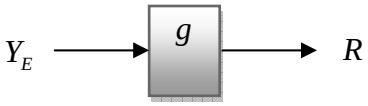
Sr is a unique number assigned to the vote.

Y_E is the encrypted Y *and* Sr.



The voter takes home Y_E and R. At home, he inputs Y_E into the system (website set up by central agency conducting the elections) and the output will be R for a correctly recorded vote. The fact that output is R should be enough to convince the voter that indeed his vote was recorded as he intended.

In other words,



where, g is the inverter function.

From DREs to Web voting

Given the stringent requirements of the voting regime, the problem of providing absolute security and verifiability is an "unsolvable problem." Since these two requirements are contradictory, a tradeoff must be adopted. Although a perfect solution may not be achievable,

solutions that are adequate in a legal sense do exist, which is where the recommendations of paper trail and open software come in.

If paper receipts brought home for verification opens the door to coercion, one may also doubt if the RNG devices, or permuters, have worked reliably. Besides intentional errors, unintentional errors will occur. Malfunction of electronic devices has been reported in the DRE elections held in the past; these included the voting machine toggling votes between parties, doubling or deleting votes and subtracting instead of adding them. There is also the possibility of unintentional behavior of programs and electronic malfunctions.

Although various levels of independent checks and supervisory programs will make electronic voting acceptably reliable, the further weak point in the system is the reluctance of the voter to stand in long lines at the voting booths. This point can be addressed only by allowing the voter to use the Web. This means that eventually protocols and algorithms of public key cryptography should be used to devise a comprehensive web-based electronic voting system. Such a system can also ensure that the voting is done only within a certain time-window that is not currently satisfied by the absentee ballots that are cast over several days before the Election Day.

Web based voting will not eliminate the basic problems of reliability; it will only shift the difficulties to higher levels in the system hierarchy. There would be greater aggregation of computational resources in the servers that will necessitate powerful supervisory agents using statistical tests to check the integrity of data at various levels. It would also require cross-checking with statistically sampled polling data.

References

1. Rebecca Mercuri. Voting-machine risks. *Commun. ACM*, vol. 35(11): 138, 1992.

2. B. Schneier, What's wrong with electronic machines? openDemocracy.com http://www.opendemocracy.net/debates/article-8-120-2213.jsp

3. David Chaum. Secret-ballot receipts: True voter-verifiable elections. *IEEE Security and Privacy*, vol. 2(1): 38–47, 2004.

4. M. Gnanaguruparan and S. Kak, Recursive hiding of secrets in visual cryptography. *Cryptologia*, vol. 26: 68-76, 2002.

Source *Ubiquity* Volume 8, Issue 6 (February13, 2007 - February 20, 2007)