Voting Protocol

Bekir Arslan

November 15, 2008

1 Introduction

Recently there have been many protocol proposals for electronic voting supporting verifiable receipts. Although these protocols have strong theoretical foundations, most current companies prefer to solve the verifiable receipt problem in a simplistic way by having the voting machine print out an untraceable vote and deposit it to the voting box after the voters examination. The electronic part is probably (details are usually lacking and the systems are proprietary) still lacking strong cryptographic privacy and security.

Putting aside economical considerations, the main reason for this seems to be the simplicity and ease of use of these systems. Ease of use is always an important consideration in complicated software systems for obvious reasons, but simplicity in this context has also an important additional advantage: it is easier to trust a system one can understand.

In the light of these issues, improving the currently used systems rather than the protocols that are theoretically sounder but are usually not employed might be more productive. To this end, we try to use methods that are used in the literature that would improve the existing systems, without reducing the stronger properties of said systems.

2 System Design Perspective

Rather than trying to improve on the work seen in the academia, the focus of our research is to build a system as complete as possible that is both practical, readily implementable by the industry and fits the related companies, government agencies and especially voters needs and preferences, but also uses the cutting edge research done by both academical researchers and companies and thereby has a strong theoretical framework.

To accomplish this we first list the basic requirements and fundamental principles along with preferable attributes. As much has been said about these issues both in technical and non-technical papers, and in government and corporate white papers and in the media, this part will be more of a organized compendium of existing ideas than original research.
After that the preferences of all the involved parties (voters, government agencies and companies) will be examined and in light of these preferences the currently marketed systems as well as academic research will be evaluated. Using existing literature and original research a new system (or possibly many) that fits all the players as much as possible will be designed.

One important issue is the assumptions made by academic researchers (usually without even knowing), and their practicality. As it is common in the security field, the most important and easily circumvented problems are not addressed while the rather inessential problems are examined to their deaths. (think of the weakest link of most security systems: the user supplied password, rather than any cryptographic or design part). Addressing these problems and analyzing them is of key importance.

3 Previous Work

A short non-technical description of the two related protocols:

3.1 Standard

This one is basically an simple but effective idea, implemented in slightly different ways (possibly with various improvements/changes) by some companies. What happens is that apart from the usual 'select your candidate on the computer' process followed by the results being sent to a central server (which basically lacks many security properties that some proposed protocols satisfy), as a paper-trail it also prints a paper-ballot of the said candidate and drops it to a box - to which the voter has no separate access. This paper ballot - which looks similar to a conventional paper ballot - is stored for a possible recount. The voter sees the ballot and confirms before it is dropped to the ballot box. In a way the system tries to satisfy correctness by ensuring the correctness of the backup vote only.

3.2 Pret-a-Voter

The main idea behind this protocol by Chaum is that the DRM never learns the vote. Basically the pre-prepared ballots have what is called an onion, which is an encrypted form of the order the candidates are listed. The user selects his candidate from a shuffled list, marks it in the voting booth, and on his way out drops part of the ballot to the voting box. The selected candidate can only be seen after the encryption is opened - which happens after an anonymizing step. The part that the voter keeps is used as a receipt - it cannot be used to prove which candidate was selected, but it can be used to verify that the correct encrypted vote was submitted to the server. The main issue with this approach is the extensive need for setting up the ballots and the implied complexity, which
causes an increase of potential pitfalls and a decrease in perceived security of the system.

3.3 Homomorphic Encryption Based Protocols

The main idea with these protocols is that votes are sent to a central server encrypted with a shared key (after a mixnet phase), and they are first combined and then decrypted. So no ballot is actually decrypted separately, which helps prevent linking of encrypted and opened ballots. These protocols were more popular before the need for verifiable receipts for a generally agreed upon requirement.

4 Major Issues with the Standard System

Consistency In the standard voting protocol, there are actually two separate votes cast. Of course the system descriptions will necessarily indicate that those two votes will always be the same, however both designing and implementing this requirement and convincing the public that this will always be the case is a problem that needs to be addressed. The reason this problem might manifest itself is closely related to the laws and rules of the election. Since voters will have visually reviewed the paper ballots, those will be the trustworthy ones. But if these are only to be used on possible recounts, in districts where getting a ruling for a recount is relatively difficult their positive effect to the reliability of the election will be diminished. This problem can trivially be solved by having the paper ballots be assigned the role of the real votes - rather than just a backup. In that case the electronic counts will acts merely as an unofficial exit poll. This however reduces the usefulness of an electronic voting scheme, so looking for a better alternative makes sense. One alternative is to ensure correctness separately, for example by using cryptographic techniques similar to ones without paper ballots. Another direction is to reduce the potential inconsistency between the electronic and the paper ballot, for instance by having a table of all the paper ballot votes indexed by their id’s, and then randomly check a predetermined amount of the ballots thereby testing if an inconsistency has occurred with a calculatable probability. This of course will need to be designed carefully, as the id’s might be used for coercion.

Coercion Resistance This problem might represent itself if it is possible to use a picture of the paper ballot as a proof. It all depends on what the system does if at the confirmation (of the paper ballot) phase the voter wants to change his vote (either because there was an error, or because of the voter changing his mind). If this process is easily recognizable by an outsider, the picture of the ballot at the final confirmation phase can be used for vote buying.
Privacy Unlike traditional voting, any electronic system which relies on the DRM to record/submit the vote has to consider the privacy issues carefully. Chaum’s protocol [1] circumvents this problem by not disclosing the vote to the DRM, but almost all other systems are at least somewhat suspect to vote recording and matching them to voters. There are a few ways to reduce the possibility of this by designing the voting procedures carefully. In case there are multiple booths (which is the case in most districts), if the public cannot see which voter goes into which booth, the probability of a successful matching of votes and voters diminishes radically. Even if all DRM’s are malicious, a confident match might be too hard. Of course this also depends on how the voter actually presents itself as a qualified voter to the DRM. Some ways that the information can be saved and later on retrieved are: by using the available storage and then make network connections, by using backdoors, subliminal channels, or similar techniques.

5 Possible Reasons for not adopting advanced cryptographic schemes

- Need for setting up a complicated and distributed mix-net. (most modern cryptographic voting protocols use mixnet for some reason or other)
- Complicated interfaces. (cut-and paste schemes)
- The belief that paper ballots are sufficient as verification and that DRM’s need to be trusted to some extent anyway. (cut-and-paste voter verification and various other schemes)

6 Protocol 1

The voting protocol is in a way a combination of Pret-a-Voter (which has the desirable property of the DRM not learning the selected candidate) and the current standard idea in the industry of having the DRM generate the human-readable ballot (for auditing purposes; these ballots are very similar to the usual paper ballots) as the only audit trail. The strength of that method is its simplicity (especially because it makes the setup reliable in the eye of the voter), but it does not use cryptography to its full strength so that the electronic votes will not be as trusted as other systems and extensive use of audit-trails will mostly defeat the purpose of electronic voting machines. Our protocol will try to combine these two systems by taking the security of the first system (thereby reducing the need for full recounts by reducing the threat levels) and the paper trail making a full recount possible and increasing the trust of the voters. Improvements include:

- Ability to have real receipt making a recount possible
• No use of ink/stamp. All done electronically (or rather by the DRM), except for possible recounts.

• Arguably easier to use.

Advantages compared to similar proposed protocols:

• Support both full recounts and full privacy.

• Relatively simple. No need to select a candidate from a big grid.

• Reduced possibility of false (or possibly false) accusations of malfunctioning. Prints choice, then asks if sure, then prints ballot and asks for confirmation.

6.1 Scenario

Voters feed a prepared ballot to the DRM. The ballot has 3 parts. The first part has (along with the onion as a barcode) the empty spots (aligned with the candidates), which the DRM will mark as the vote. The second part has the candidates listed in a random order. The last part has the human readable onion - which works as the id of the ballot. It will be used to map the marks to the candidates. The user feeds the ballot to the DRM. At this stage only the first part will be inside the DRM, until the voter selects the spot he wants to be marked (not directly the candidate - so the DRM won’t know which candidate is selected). After he confirms his choice, the printer will print the receipt and submit the vote to the server. This part will be very similar to Pret-a-Voter. It will then take the second (un-separated) part and leave the third part for the user. The first and second parts together will be the paper-trail - making it possible to have a recount.

6.2 Details

The math behind the onion is very similar to Pret-a-voter. But there are some differences. Firstly, since there will be paper ballots for possible recounts, some requirements might be relaxed. Secondly (and more importantly), one needs to make sure that the DRM actually marks and submits the correct number as the selected candidate. (As there will be one electronic and one paper vote, both of these should be verifiably correct) This will mostly be easily checked by the voter, but care must be taken to prevent the DRM from possible cheatings. The key part is to make sure that the selected number will be the same as the actual choice - which will mostly be the voter’s responsibility. After the voter selects his choice, and the DRM marks the spot, it also prints the first part of the receipt. This receipt will also include the selected order, and so in a way this receipt will include all the information of the printed receipt and ballot leftover part from Pret-a-Voter.
6.3 Security

Some possible issues that need to be analyzed in detail:

- Making sure that the submitted electronic vote is correct and private - particularly there should be no way the DRM can construct a correct vote on his own. This is mostly taken care of by the Pret-a-Voter part.
- The paper ballot should be correct and the same as the electronic vote. This is checked by the user, who can alert authorities if a mismatch occurs.
- Matching the receipts with the paper-ballots should be impossible (or at least difficult). This property is currently not satisfied - but it should be possible to do so.
- To prevent the $V_D$ from reading the candidate order, fonts that are difficult to read by scanners can be employed.
- Write-ins might be added, but they will be non-trivial to use.
- Specially marked ballots might be used for coercion. To prevent this one might let the $V_D$ print a copy of the receipt part of the ballot and keep the original.

7 Protocol Details

7.1 Participants

Authorities The authorities $A_1 \ldots A_m$ will be responsible for the keys that encrypt the final votes.

Voting Device The Voting Device $V_D$ gets the votes from the voters and submits them to the $BB$. $V_D$ uses a computer screen $S$ to display information to the voter. It also uses a printer to print a receipt $R$ for that purpose. The difference of these is the fact that $D$ will remain secret between the voter and the voting device, whereby $R$ will be taken outside the booth by the voter.

Voter The Voter $V$ uses $V$ to submit a vote for his selected candidate.

Bulletin Board The Bulletin Board $BB$ is where the $V_D$ submits the votes. It is publicly readable, and write-only for the $V_D$. $A$ will read the votes from here.

Coercer The Coercer $C$ is a hypothetical participant.

7.2 Setup

Each authority generates its public/private key pair and publishes its public key $PK_i$. 
7.3 Voting

This phase occurs inside the voting booth, so it is assumed that there is a private and secure channel between V and VD. The only information that will be revealed to an outside party is the vote submitted to the BB by VD, and the receipt R printed by VD.

1. VD displays a $d \times n$ matrix, where $d$ is a security parameter, and $n$ is the number of candidates (including a generic ‘write-in’, and a possible abstain). Each row in this matrix consist of these candidates in a random order.

2. VD also prints a commitment for this matrix, using a one-way hash with random salt. This salt will be revealed when the commitment needs to be opened. (The commitments can be based on each entry or on each row)

3. V first randomly choses a row, and then submits his chosen row and column (and thereby candidate).

4. After the candidate selection, VD opens the commitments for unchosen rows by printing the random numbers used for the commitment. It also prints the selected row and column, but not the name of the candidate.

5. If the candidate was ‘write-in’, V uses the write-in ballot to print the encrypted name and the onion.

8 Protocol 2

This protocol is a combination of classic homomorphic encryption schemes, and the standard method. Unlike the previous protocol, the VD will have the voting information, but to prevent cheating the cut-and-paste method will be used. As an advantage to the previous method, no paper ballots will be necessary to vote, the final paper ballot and the receipt will be printed by the VD. The only additional burden (for to the voter) would be the need to select the preferred candidate from a grid. This might be confusing for some users, but even very simple initial instructions would make it easy to use for the average voter. The advantage would be the extra certainty that the electronic vote counted as intended.

8.1 Comparison

8.1.1 Comparison with Pret-a-Voter

- A paper audit-trail. Votes can be recounted.
- The candidate list is needed, so it cannot be kept (and potentially used for vote buying etc). The design is such that even if the DRM reads the list (since it will have the hardware necessary for it - to be used for
reading the barcode), the design insures that the commitments (pretty much everything that will be submitted to the server) are already printed, as is the paper vote itself.

8.1.2 Comparison with Standard

Almost everything that Pret-a-Voter can do compared to Standard, this protocol can do. This mostly includes greatly improved privacy, voter verification of the electronic vote, and again greatly increased correctness.

9 Possible Future Work

1. Extensive listing, description and valuation of potential security and other problems with the standard system.
2. Propose potential solutions for these issues.
3. Complete the detailed descriptions of the two proposed protocols.
4. Simplify the homomorphic encryption based system (with voter-verification support).
5. Improving the consistency of the electronic and paper ballots in the standard system.
6. Simplify the Chaum protocol combined with standard paper ballots.

References