How to defeat Rivest's ThreeBallot Voting System

Andrew W. Appel
Princeton University

October 5, 2006

Abstract

Rivest's ThreeBallot voting system is proposed as a method that is secure against either vote-buying or miscounting. However, it is not secure against both vote-buying and miscounting together.

1 Introduction

Secure voting systems are difficult to design, because they must ensure both the accuracy of the count and the secrecy of the ballot. The secrecy of the ballot must be extremely strong—even with the full cooperation of the voter, the cheater must not be able to learn how the voter voted. If the voter can prove how she voted, then she can sell her vote, or be coerced into proving how she voted (and thus, coerced into voting a certain way). Vote-buying (and by symmetry, vote-selling) has a long history in our Republic; it tends to be concentrated in corrupt districts and is practically nonexistent in other areas, which is why some people have difficulty believing it really exists. Often vote-buying is found in the same corrupt districts as wholesale fraudulent miscounting. See the excellent history by Campbell [Cam05] of the amazing prevalence and persistence of both miscounting and vote-buying in the United States.

The Australian secret ballot—a preprinted form marked by the voter, deposited in a ballot box, and counted when the box is opened in the presence of witnesses from both sides—was invented in the late 19th century as a mechanism for simultaneously guaranteeing the accuracy of the count and the secrecy of the ballot. However, this system is still vulnerable to attacks if not implemented well. In some places there are not enough witnesses from both parties to be found to watch the count; or the people handling the ballots during the count can keep pencil-lead under their fingernails to mark ballots as they are counted; or the witnesses can be coerced; or the ballot boxes can be stolen and then reappear; or the ballot boxes can be switched in the middle of the election day during a moment of inattention by the pollwatchers; or fifteen other ways to cheat that are well documented. The remarkable thing is that some of these methods are so blatant that "everyone" must know they're going on, but that doesn't always prevent them.

There have also been many successful attacks on the secrecy of the Australian secret ballot: chain voting; political party hacks accompanying voters into the booth; voters showing their ballots to the party hacks before depositing them into the box; voters putting a special mark on their ballots so they can be identified during the count. Again, many of these methods are blatant, but some are not.

Though the paper ballot is vulnerable to these frauds, purely electronic methods commercially available now and in the foreseeable future—that is Direct Recording Electronic (DRE) voting machines and Internet voting—are *more* vulnerable to both kinds of fraud. Computers can *and do* keep a record of the votes in the order that they are cast, compromising privacy, and computer can *and have been* programmed to change the votes in their memory during the casting of the vote [FHF06]. No witnesses from opposing political parties can watch the voting machine recording the votes in its internal memory.

2 Three-ballot voting

Rivest [Riv06b] proposes a system for voting on paper that, he claims, protects the auditability of the count by ordinary voters and still guarantees ballot secrecy. To simplify the explanation of his system, I will assume there is only one race on the ballot, and only two candidates in that race, Alice and Bob.

The voter is given three ballots, which are identical (listing Alice and Bob) except that each has a different random, hard-to-remember serial number on the bottom. Suppose the voter wants to *vote* for Alice. On exactly two of the ballots she *marks* the spot for Alice; on exactly one of these ballots she marks the spot for Bob. On a given ballot there might be a mark for Alice, or a mark for Bob, or both, or neither, but the totals add up to two-and-one.

She feeds the three ballots to a machine which verifies that she has voted exactly two-and-one (and not three-and-zero). She then chooses one of the three ballots, and is given a copy of that ballot (complete with serial number) to take home; meanwhile, all three ballots are deposited in the ballot box.

At the end of the day, a copy of every ballot, complete with serial number, is posted on a public "bulletin board" (on the Internet in a convenient machine-readable form). Anyone can add up the marks; if n voters voted for Alice and m voted for Bob, there will be $2n + m$ marks for Alice and $n + 2m$ marks for Bob. If more voters wanted Alice, then $n > m$ and therefore $2n + m > n + 2m$, and Alice will win.

Suppose an insider cheats: after the voter has voted but before the ballots are posted, the insider changes a mark on a ballot in the ballot box. For each such changed ballot, there is a 1/3 chance that the voter chose to take home that receipt.[1] The voter can check the bulletin board to make sure that her ballot is present (it is identified by its unique serial number) and has not been changed. She even has proof of how she marked *that ballot* which can be used as evidence. She does not have proof of how she marked the other ballots; for two-thirds of the ballots in the box, no voter has a receipt.

On the other hand, suppose Bad Bob's party hacks want to coerce voters or to buy votes. They make it known that they will pay $100 for every "Bob" receipt (i.e., for every receipt showing marks for Bob and not for Alice). In a naive voting system with actual receipts, where the voter could use the receipts to prove how she voted, then this is a good deal for the voter and for Bob—but presumably a bad deal for the public at large and for the integrity of the democratic system. In Rivest's method, the voter can mark (twice) for Alice (and once for Bob), then take home the receipt for Bob and collect her $100. This is a good deal for the voter, but not for Bob, who gains nothing.

Because the voter cannot prove how she voted, the system is secure against vote-buying and coercion—except that it is still vulnerable to all all the blatant methods that have been so prevalent historically! That is, Rivest's method is no more secure against vote-buying than is the Australian secret ballot. On the other hand, Rivest's claim is that his method is secure against fraudulent miscounting.

3 Usability problems

Strauss [Str06] describes a dozen different problems with three-ballot voting. Many of these problems are extremely serious, rendering the system unusable or insecure.

For example, in many localities, there may be up to 70 races on the ballot, each with the possibility of more than 2 candidates. Under current practice, if the voter marks the 5 races of interest to her, she has constructed a valid ballot. A precinct-count optical scan machine may warn her that she has undervoted, but she is free to ignore that warning and cast the ballot anyway. If she overvotes in one race—rendering her vote in that race invalid—a precint-count optical scan machine will warn her of this, and give her a chance to void this ballot and mark a new one. But she is free to ignore the warning, in which case her vote *in that race* will be void but her votes in the other races will be counted.

But with the three-ballot system, it is absolutely not permissible to undervote or overvote. A ballot that is invalid in one race *must not be cast*. But a 70-race ballot with several candidates in each race requires the voter to place hundreds of marks, and do so accurately. Evidence already shows that several percent of voters have difficulty placing 20 or 50 marks accurately—but at least the ballots of those voters can be counted in all the races that they don't mess up. With three-ballot voting, many voters will be extremely frustrated.

With conventional precinct-count optical scan voting, if the machine breaks down during the election, voters can still mark ballots and put them in the ballot boxes to be counted later. With three-ballot voting, if the machine breaks down there is no way that polling officials can accept triple ballots.

4 Security problems

Strauss also points out many security problems with Rivest's scheme. Many are inherent in the notion that the voter must check the serial number of *one* of the three ballots to make sure it matches the receipt, but cannot remember the serial number of the other two ballots. It is not at all clear that this notion is realistic, especially in the era of camera phones.

Other security problems are caused by the fact that voters can leave the polling place with marked and "approved" (red-striped, in Rivest's terminology) ballots. Rivest says they cannot do this, but election workers know that voters do in fact forget to put their ballots in the ballot box, and the voters cannot be physically restrained from walking out of the polling place with their ballots. See Strauss [Str06] for an explanation of these attacks.

Receipt buying. One of the problems Strauss discusses is attack called "receipt buying." Bob cheats by buying "Alice" receipts. For each one, he can safely change the corresponding serial-numbered ballot in the box from an Alice mark to a Bob mark, because the voter no longer has the receipt to prove anything. Rivest points out that the voter can prevent Bob from doing this by keeping a copy of her receipt. Rivest suggests several methods that might make it easier for voters to

[1] Discussions of voter-verified paper ballot using the Mercuri method often misuse the word "receipt;" in that method the voter does not *receive* the printed ballot, but instead that ballot is deposited in a ballot box. The word "receipt" often causes confusion and should not be used in connection with the Mercuri method. Here, however, it is just the right word.

have multiple copies of their receipts, to prevent receipt buying.

5 A combined attack

The fraud I will describe here is quite a different kind of receipt buying, and works even if voters can keep their receipts. Bob will pay (or intimidate) to see *marks for Bob*, not (as in the receipt-buying attack Rivest considers) marks for Alice.

Bad Bob makes it known, quietly but in a way that everybody knows,[2] that his guys will pay $100 for every Bob-receipt that they are shown (that is for every receipt that shows a mark for Bob and no mark for Alice).

The election is divided into precincts, with one ballot box per precinct. The vote totals reported for each precinct.[3] In New Jersey, for example, there are about 600 registered voters per precinct, and with a 50% voter turnout we can expect 300 voters to come to the polls.

In a particular precinct, 300 voters go to the polls: $n = 175$ vote for Alice (two ballots marked for Alice, one for Bob) and $m = 125$ vote for Bob (two ballots marked for Bob, one for Alice). Almost all of these voters (both Alice and Bob voters) are motivated by either money or intimidation to bring out a receipt that Bob will like, so they make sure that one of their ballots has 1 vote for Bob and 0 votes for Alice—this is a "Bob receipt." In addition, Bob asks his own partisans to vote in the pattern (Bob, Bob, Alice) and not in the pattern (Bob+Alice, Bob, none); a substantial fraction of the m Bob votes contain a ballot marked just for Alice.

Bob's guys pay $100 for every Bob receipt they are shown (Bob himself stays out of it, as he's a respectable office-seeker). Only $a = 30$ voters take home a receipt showing an Alice vote, and of those only $f = 1/2$ will bother to check the bulletin board.

Now there are $3(n + m)$ ballots in the box; on these ballots there are $2n + m$ Alice marks and $n + 2m$ Bob marks. Before committing their fraud of changing a few votes in the box, Bob's guys have a good estimate of how many non-Bob receipts are out there. They've seen almost 270 Bob receipts—even from Alice voters—and there are at most 300 receipts out there.

Bob's guys decide to change $c = 50$ ballots from Alice to Bob—that is, on ballots that showed 1 mark for Alice and 0 for Bob, they change the ballot to show 0 for Alice and 1 for Bob. After they do this it appears that Bob has beat Alice in this precinct by 175 to 125. The voters check their receipts against the posted results, and don't find any fraud. That's because they've been bribed or coerced to keep only their Bob receipts. But Bob doesn't alter any of the Bob-only ballots—those are already marked for him, and those are the ones on which changes would be most likely detectable, because voters have receipts for them!

There are $a \cdot f = 15$ voters who kept their non-Bob receipts and will actually bother to check the bulletin board. But Bob altered only c ballots, out of a total of $2n + m$ Alice ballots.

The probability that he altered one of those for which a receipt was kept is only about

$$1 - \left(1 - \frac{a \cdot f}{2n + m}\right)^c$$

or in this case, about 35%. Bob has a 2/3 chance of getting away with it, in this precinct.

Bob needs to steal more votes than just the 26 needed to win in this precinct, because in some other precincts he hasn't been able to buy enough receipts to safely change any marks. Bob can change marks in any precinct where he has seen enough receipts to be confident that there are very few Alice receipts extant (and in which he has physical control of the ballot boxes).

The combination of massive receipt-viewing with count-tampering removes a critical assumption that Rivest implicitly relies on. In effect, the voter can't sell her vote. But she *can* sell away her ability to audit (her portion of) the count.

6 Bob gets caught—so what?

Bob may need to perpetrate this fraud in several precincts. Suppose he changes 50 votes in each of 5 precincts; then there is almost a 90% chance that *one or two* extant Alice-receipts will not match the corresponding vote on the bulletin board. But there will be no massive pattern of changed votes—just evidence that one or two votes didn't match the receipt. History shows that judges are already very reluctant to overturn elections even when massive fraud is convincingly demonstrated. No judge will overturn an election on the basis of one demonstrably fraudulent ballot, especially if Bob makes sure he wins by 10 or 20 votes. It will be impossible to convince the judge that 1 *detected* changed ballot means, statistically, that many more votes must have been changed.[4]

[2] This seems like a contradiction but, in fact, that's the way it works in practice.

[3] This is the standard practice in American elections, for very good reasons. It is helps ensure that the number of votes in each precinct is equal to the number of voters in that precinct, which in turn is not greater than the number of registered voters in that precinct. Per-precinct totals will necessarily arise when a ballot box is opened and counted in front of witnesses.

[4] I assumed that of the a voters that walked out of the polls with their Alice-receipts, only some fraction f of them would actually keep the receipts and check them against the bulletin board. Rivest suggests [Riv06a] that after one or two changed ballots are detected (because one of the Alice-voters checked her receipt against the bulletin-board), the lawyers for Alice can search for more voters; that is, there's a pool of a receipts out there, not just $a \cdot f$. But this will just mean that instead of evidence of 1 or 2 changed ballots, there will be evidence of 3 or 4. Of all those 30 Alice-receipts, *the vast majority them correspond to ballots that Bob did not change.*

It might seem that a 90% chance of some evidence showing up might not be very attractive for Bob. But of course, historically, where vote-buying is prevalent, it's no secret. Upon reflection, this cannot be too surprising: Bob cannot buy massive numbers of votes without massive numbers of people knowing about it.

Here Bob is not even buying votes—he is just asking to view receipts. The massive evidence is only for the receipt-viewing, not for the vote-changing. But requesting to view the receipts of ordinary voters is not meant to be illegal: Rivest envisions that of voters will give their receipts over to "helper organizations" (such as their own political parties), who can perform the bulletin-board checking in an organized way. Bob's guys are just "helping."

7 Conclusion

Conventional paper-ballot voting (or optical-scan voting) already uses several (imperfect) defenses against unauthorized changes of ballots after they are cast. Rivest has proposes three-ballot voting as an additional defense, not to replace the existing defenses [Riv06a]. We should consider three-ballot voting as an additional imperfect layer of defense, and if it is weak at *different* points than the other layers then it will be worth considering.

Rivest's paper (as of October 1, 2006) includes discussions of possible attacks and of usability issues, and he proposes countermeasures to those attacks and polling-place procedures that are supposed to mitigate the usability issues. The attack I have described is just one more on top of the many attacks he describes. Perhaps it is possible to design countermeasures to this one—Rivest suggests [Riv06a] offering a $1000 bounty to any voter who turns in a receipt that proves the bulletin-board was compromised. Of course, there are attacks on this countermeasure—even if Bob doesn't choose to change votes wholesale, he can sow confusion and collect a quick $1000 by changing just one Bob mark to an Alice mark! The point is that layering enough countermeasures makes ThreeBallot voting very compex indeed.

ThreeBallot voting is subject to many usability problems, which are probably more devastating and significant than the security problem I have described, but they are beyond the scope of this paper.

In conclusion, the weaknesses of three-ballot voting do not coincide exactly with those of conventional ballot-counting, so three-ballot voting does provide additional protection. But the amount of additional protection is not enough to justify its extreme cost in usability and complexity.

References

[Cam05] Tracy Campbell. *Deliver the Vote: A History of Election Fraud, an American Political Tradition—1742–2004*. Carroll and Graf, New York, 2005.

[FHF06] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. Security analysis of the Diebold AccuVote-TS voting machine. itpolicy.princeton.edu/voting, September 2006.

[Riv06a] Ronald L. Rivest. e-mail communication, October 2006.

[Riv06b] Ronald L. Rivest. The threeballot voting system. http://theory.csail.mit.edu/~rivest/Rivest-TheThreeBallotVotingSystem.pdf, September 2006.

[Str06] Charlie Strauss. The trouble with triples: A critical review of the triple ballot (3ballot) scheme, part 1. http://www.cs.princeton.edu/~appel/voting/Strauss-TroubleWithTriples.pdf, October 2006.