Securing the Vote: Electronic Voting in Theory and Practice

Mallory Grider

December 12, 2018

Abstract

The 2000 U.S. presidential election recount in Florida spurred interest in the possibility of remote electronic voting. With the accessibility of the Internet, and inability for electronic voting to produce a “hanging chad”, voting online seems like a promising substitute for old-fashioned paper ballots. However, voting via the Internet poses serious security risks that can undermine both the voter’s ballot and the election cycle. This paper aims to provide a survey of how technology can properly be utilized to secure elections. To do this, we examine three theoretically secure voting systems: STAR-Vote, David Chaum’s Vote Verifiable, and Ron Rivest’s revised Three-Ballot voting. In the investigation of these three protocols, this paper considers how to ensure the credibility of a vote at the physical polls vis-à-vis cryptographic and digital means.
1. Introduction

The 2000 U.S. presidential election recount in Florida spurred interest in the possibility of remote electronic voting. With the accessibility of the Internet, and inability for electronic voting to produce a “hanging chad”, online voting seemed like a promising substitute for old-fashioned paper ballots. Internet voting promised increased voting participation and exact counting. As recent as 2016, California proposed two ballot initiatives to launch internet voting.¹ However, as stated by David Dill, professor of computer science at Stanford University, “From the perspective of election trustworthiness, Internet voting is a complete disaster.”² While it is impossible to guarantee the security and privacy of an Internet election, technology does deserve a place in the polls. The future of voting lies in an amalgamation of new and old; instead of completely replacing the paper ballot, all promising endeavors to secure public elections involve a mix of in-person polling, electronic verification, and safe cryptographic protocols. Unlike a computer, paper cannot be hacked.

This paper seeks to answer how technology and theory can be used to buttress public elections. To this end, we will examine three voting methods designed to improve the security of elections: the STAR voting system, David Chaum’s Vote Verifiable Scheme, and Ron Rivest’s Three-Ballot Voting.

2. To the Community

Secure voting secures democracy. This paper will define a “secure” vote as follows: all votes were counted and each vote can be verified that they were counted, an attacker cannot falsify or alter any vote, all votes were cast in secret, and all eligible voters voted only once. By proving to voters that their vote counted, and that the election outcome is in accordance with the votes cast in favor of the winner, the winning party is legitimized. Within the past 5 years, we have witnessed egregious vulnerabilities in domestic and international elections; these cases include, but are not limited to, Russian tampering in the U.S. presidential election in 2016, the release of absentee votes via Excel sheet by the Georgia Secretary of State, Brian Kemp, in 2018, and the MongoDB breach of 93.4 million Mexican voters’ private data in 2016.³ Learning about the practices that contribute to voting security heightens public perception and knowledge of their election systems.

3. Secure Voting Methods - STAR Voting

The sales volume of the first true electronic voting system, the Direct-Recording Electronic voting system, surged after 2000. However, the DRE was proved insecure by John Hopkins University professors Avi Rubin and Dan Wallach in 2003. This finding launched the research that led to the STAR-vote system, an acronym for “Secure, Transparent, Auditable, and Reliable.” Like DRE, STAR relies on an electronic voting machine. The voter interacts directly with a GUI to cast their ballot. The physical machines are quite similar, but the end-to-end cryptography employed in STAR is different than the traditional DRE.

The voting protocol for STAR-vote is straightforward for the user. The voter receives a 1D barcode that encodes their precinct and ballot style. The voter presents the barcode to a polling place employee, who scans the barcode and prints a receipt with a unique, 5-digit code. The 5-digit unique code is only in use for a short period of time for a limited amount of ballot terminals and voters, and so the risk of collision between codes, or brute-forcing a valid code, is minimal. There is no memory of the one-time-use code in the STAR system, and so an attacker cannot internally access any of these digits. The voter takes this code to a machine, inputs their code, and selects their choices. After their selection, the machine provides a summary of their vote and a receipt. The summary is deposited into a ballot box by the voter, and the receipt can be used to verify that their votes were counted via a public, online “bulletin board”. The ballot box only accepts the summary if it matches the expected ballot ID, ensuring that only the correct vote is counted. The user receipt contains the hash (16-20 characters) of the ciphertext of their vote, which is used for reference on the web bulletin board; by nature of a hashing function, this ensures that the receipt code has no conflicts with any other vote.

STAR-vote relies on a threshold cryptosystem; the officials monitoring the system and the voter all must handle elements of the system that encrypt and decrypt a vote. Furthermore, each STAR-Vote machine communicates within its local network to dictate the 5-digit ballot code and the 16-20 digit post-vote hash value for a particular vote. The hash value for a particular vote is computed as follows:

$$z_i = H(E_k(v), m, z_{i-1}) \text{ where } i = 0, ..., n$$

where H denotes the hash function, E denotes encryption, m denotes a single machine, v specifies the voter’s selections, k is threshold value, and $z_i$ is the hash result for that particular vote ($z_{i-1}$ is the previous hash that came from that machine). Votes are stored within the system.

---

5 Ibid.
7 Ibid.
in their encrypted form. Decryption keys are not kept within the STAR-Vote system, and so no attacker can obtain these keys by hacking any one machine. Confidentiality is maintained because neither the ballot summary nor the receipt reveals voter identity. Election integrity is checked by the homomorphic tallying process and voter receipt.

STAR-Vote is a marriage between technological interface and paper; the system allows for the utilization of electronic voting equipment while also providing a physical paper trail of election results. However, STAR-Vote is not flawless. Physical machines can be stolen or broken. The ballot summary printout contains information about voter selections, and as such, the ballot box could be a target for tampering. And it is only a matter of time before any hashing algorithm is cracked.

4. Secure Voting Methods - Vote Verifiable Scheme

Like STAR-Vote, David Chaum’s Vote Verifiable Scheme is predicated on the idea that each voter should be able to confirm that their vote was counted in the election. Unlike STAR-Vote, Chaum relies on visual cryptography to encode a vote on a receipt, not a hash function.

Under Chaum’s Voter Verifiable Scheme, a voter casts their ballot on a GUI. The machine generates a receipt with a textual image of their selection, which the voter is asked to confirm. This human-readable image will not leave the polling booth. The voter selects one of two possible “layer” images that, together, compose the image they originally confirmed. Under each of the two images is a unique barcode. The voter receives a printed, transparent copy of both images and is directed to a voting official. The layer marked for surrender is torn off and given to the official. With the surrendered layer, the official checks that it is the counterpart to the one kept by the voter, and that the vote was effectively tallied. The surrendered layer is promptly shredded. The layer kept by the voter is deemed their receipt, and an electronic version is kept within the voting system until the end of the election. With this receipt, the voter has the ability to check online that their vote was counted. Trustees of the system decrypt the layer to tally the vote. All decrypted versions of the vote can only be linked to a ballot ID, not an individual. The final receipt contains no information about the voter’s identity or decision.8

Throughout the process, anonymity is maintained through the visual encoding of the vote, represented in the two printout “layers.” These images appear as a seemingly random array of tiny black and white pixels, which, when overlapped, display voter ID and their vote (the so-called “ballot image”).9 A visual XOR of the two overlays reveals the voter’s selection. A matching symbol lets light through, revealing the vote to appear greyish, while a non-matching pattern is completely opaque.10 That is, to represent area that is not voter data, the two layers are inverses of one another; where one pixel is black on one image, the other is white on the

9 Ibid.
surrendered image.\textsuperscript{11} The protocol that creates these images is like a hash function in that Chaum’s scheme guarantees no image “collision” between shared keys (i.e. the white pixels of the voter’s selection). This process of generating the visual overlay, essentially a binary matrix, relies on One-Time-Pad. Provided randomization, mathematician Claude Shannon deemed One-Time-Pad the only unconditionally secure encoding algorithm in the late 1940’s.\textsuperscript{12} However, the process of receipt encoding is not purely random, and thus, can only be called computationally secure. To everyone but the trustees of the system, the formulation of white pixels relative to the ballot image is nearly indistinguishable from random.\textsuperscript{13}

At every stage of the ballot process, coercion and vote buying are prevented by concealing all instances of voter identity and ballot decision. If a malicious party commandeers a receipt, the most that they can glean from the presence of a white pixel is that either it forms the “grey space”, comprising voting data, or that it’s counterpart is a black pixel that forms opaque space (and hence reveals no sensitive information). Integrity is maintained by virtue of the receipt, which allows for end-to-end auditing by voters, election officials, and trustees of the system.

The chief criticism of the Vote Verifiable Scheme was made by its inventor, David Chaum, who criticized the scheme’s inability to monitor behavior within the polling booth. In the IEEE Computer Science journal, Chaum remarked, “Even the ‘gold’ standard of voting systems - paper ballots - is subject to marking or ballot number recording.”\textsuperscript{14} Chaum’s scheme, for example, relies on the surrender of the second layer for shredding. This action requires human intervention, arguably the most unstable algorithm known to exist.

5. Secure Voting Methods - Three-Ballot Voting

Unlike Vote Verifiable Scheme and STAR-Vote, Ron Rivest’s Three-Ballot Voting does not require an electronic machine for the voter to cast their ballot. Rather, Three-Ballot relies on the “gold standard” referenced by Chaum – paper. Rivest’s paper ballot is arranged along three columns, with each column containing an identical list of the candidates. Voting happens along rows; to vote for one particular candidate, between all three ballots, two bubbles must be filled along their row. To vote against a candidate, or to abstain from voting for a candidate, the voter fills in only one bubble. In either of these two scenarios, it is at the voter’s discretion to choose which bubbles to fill. A ballot with three bubbles filled across a row or that contains an empty row will be automatically rejected.\textsuperscript{15}

\textsuperscript{11} Chaum, David, Peter Y. A. Ryan, and Steve Schneider. “A Practical, Voter-Verifiable Election Scheme.” In In European Symp. on Research in Computer Security, Number 3679 in LNCS, 118–139. Springer-Verlag, 2005.
\textsuperscript{13} Chaum, David, Peter Y. A. Ryan, and Steve Schneider. “A Practical, Voter-Verifiable Election Scheme.”
\textsuperscript{14} Chaum, David. “Secret Ballot Receipts: True Voter-Verifiable Elections.”
A “checker” machine validates the voter’s bubbling, and prompts the voter to select which of the three ballots they would like to take home as a receipt. The machine prints a copy of the selected ballot, and the original ballot (but with the three perforated columns separated) is deposited into a ballot box. An electronic record of every ballot is recorded and published onto an online web bulletin. The bulletin also includes a list of names of everyone that voted in that election. The voter checks that her name is recorded and that there is a ballot matching the receipt that she chose at the checker.\textsuperscript{16} There must be exactly three times the number of ballots on the page as there were voters. The votes are listed in a public forum in plaintext, so anyone with access to this bulletin can tally the total votes. For instance, if we have candidate Bob and Alice, with \( n \) voters, their tallies are calculated as \( n + B \) and \( n + A \). Subtract \( n \) from each respective total to receive each candidate’s final vote.\textsuperscript{17}

Rivest’s method uses neither a formal hash function nor computational cryptography, but insists that election integrity and ballot secrecy is preserved. Integrity is safeguarded since there is no way to identify a voter by a specific ballot on the bulletin. Furthermore, if an attacker is to tamper with the board, they have to attack both the list of names and the ballots, otherwise a voter will file a protest about the state of the bulletin. For the case where an attacker tries to buy a vote according to a specified pattern (that is, they dictate to a voter how to mark the three-ballot), Rivest proposes either using a DRE machine or randomly filling in one row on every ballot to prevent this attack. In the case of ballot secrecy, even if the voter were to try to convince an attacker how they voted, they would be unable to because their receipt cannot reveal which way they actually cast their ballot; they could be holding their real selections, or a copy of one of the other “no” ballots.

There is an important caveat to Ron Rivest’s original voting scheme: Three-Ballot Voting is, in fact, insecure. In 2006, Charlie Strauss of Los Alamos National Laboratory published a two-part report, “The Trouble with Triples”, proving that vote buying is possible under the Three-Ballot system. In his report, Strauss concedes that Three-Ballot is secure if there are only two possible choices on the ballot.\textsuperscript{18} For more than two candidates, however, an attacker can reconstruct, with some degree of certainty, the ballot cast given a voter’s receipt (violating ballot secrecy). The attack relies on the fact that the ballot is cast in triples. A series of ballots on the bulletin with three votes or zero votes cast in a row cannot have been from one voter (by virtue of the system’s rules). An attacker eliminates these ballots, and with \( O(n^2) \) complexity, can determine a finite intersection set of possible cast ballots.\textsuperscript{19} In a simulated election of 7 races, each with five contestants, and 30,000 cast ballots, when a voter is affiliated with a major party, Strauss’ Python program accurately cracks their ballot from the bulletin name list 90\% of the time.\textsuperscript{20} In response to this attack, Rivest\textsuperscript{17} suggests using a DRE machine or randomly filling in one row on each ballot to prevent ballot buying. Strauss\textsuperscript{18} writes that this attack can be prevented by ensuring that the bulletin includes a list of names, so each voter can verify their ballot was cast correctly.

\textsuperscript{16} Ibid.
\textsuperscript{17} Ibid.
\textsuperscript{20} Ibid.
to these findings, Rivest revised the Three-Ballot system to include unique identifiers at the end of each ballot.\(^\text{21}\)

### 6. Application

In 2018, due to lack of industry support, the county department that prompted the research that led to STAR-Vote temporarily halted their efforts to get the STAR network out in a real polling place.\(^\text{22}\) For a voting protocol to be completely effective, it must go through field testing. None of the systems listed have been implemented in an actual election or even a live simulation. The STAR-Vote machine requires software licensing and new voting terminals, both of which are costly. Even though Chaum and Rivest’s schemes can use existing infrastructure, election administrators do not want to pay to transition to new software and printouts. The learning curve is also steep; in the case of Vote Verifiable and the revised Three-Ballot, the responsibility to learn how to use the new ballots rests solely on the voter. What were to happen if a cohort of voters accidentally thought that, to select a candidate, they filled two holes along a row, instead of one? The election results would not be considered valid, because “voter intent” could not absolutely be determined.\(^\text{23}\) Testing in a live simulation, then subsequently in a small election, would allow these mistakes to be effectively diagnosed and mediated. It is for these reasons that Travis County of Texas should endeavor to integrate STAR-Vote into local elections, and ballot-only states like Massachusetts should attempt the revised Three-Ballot. Since local county elections are deemed less high-stakes than federal elections, the process should begin by implementing the paper-only secure voting options in counties that already use paper-only ballots.

### 7. Conclusion

In response to Russian hacking of the 2016 U.S. presidential election, the National Academy of Sciences established a committee designed to draft proposals for improving nationwide election security. The committee deemed that “Internet voting should not be used at this time” and that “elections should be conducted with human-readable paper ballots.”\(^\text{24}\) The committee qualified it’s latter recommendation, stating that machines can be used to verify, randomize, and print such ballots. STAR-Vote, Vote Verifiable, and Three-Ballot do not use the Internet. All three systems rely on human-readable ballots with receipts. If true election security is to be obtained, the first step is to follow the recommendations of this committee. We must look to existing theory, and move towards implementation, to avoid yet another 2000, 2016, or 2018.

Bibliography


http://search.proquest.com/docview/2086667532/?pq-origsite=primo.


“Georgia’s Secretary of State Brian Kemp Doxes Thousands of Absentee Voters.”


