

## A Better Way to Vote

Charles A. Gaston  
*Penn State - York*  
*cag9@psu.edu*

### Abstract

*The Florida election fiasco of 2000 has produced thousands of articles about the problems with voting technology, hundreds of ideas how to fix those problems, and one radically different voting system that reasonably can be claimed to be both more secure and less expensive than any other system in existence. Security is obtained not by secrecy, but by extreme openness. Low cost is obtained by basing the system on hardware that is literally free. (This system, if adopted, also would be good for the environment.)*

### 1. Introduction

The outcry to “fix” our election systems began even before the winner of the 2000 presidential race was determined. Estimates of the cost of doing so ranged into the billions of dollars [1]. Direct Recording Electronic (DRE) systems were considered the favorite for replacing older types, but they tended to cost about \$5000 per voting station. Florida spent about \$32 million on a variety of upgrades, particularly replacing the notorious punch-card systems; Georgia spent about \$54 million converting the entire state to one type of DRE system [2]. Maryland signed a contract to copy what Georgia did [3]. Meanwhile, various individuals and groups were becoming louder and more insistent about the dangers of trusting something as important as voting to proprietary (read “secret”) machines, offering no way to verify correct performance, produced by a very few companies [4], [5].

The 2002 election in Georgia produced at least two significant upsets, raising the level of suspicion or paranoia (take your pick) [6]. Obvious system failures (vote totals that could not possibly be correct) and illegal last-minute software changes have added ammunition for those demanding something better [7]. Perhaps the most damning incident was when software for the machines used in Georgia was discovered on the internet and analyzed by computer security experts. They revealed hard-coded passwords and encryption keys, insecure card-reader systems, comments indicating unresolved bugs, and other poor programming practices [8]. Now there is a growing movement to require voter-verified paper ballots with every voting system [9].

A significant effort still exists in trying to make internet voting secure [10], and states such as Arizona and Alaska have tried it [11]; however, many consider that approach to have a completely unacceptable risk. It would have great advantages for the military, simplifying the process of voting from overseas, but the potential dangers caused that plan to be dropped [12]. A company touting completely secure internet voting revealed an embarrassing hacker intrusion [13]. The possibility of having a U.S. election outcome determined by a lone individual from anywhere in the world makes this approach scariest of all.

Numerous people have accepted as fact, and are acting on, the proposition that a voter-verified paper ballot is essential for a “clean” election [9]. This paper attempts to reveal a better way.

### 2. History: concept and early development

The extremely high cost estimates for upgrading the nation’s voting technology led the author to envision a voting system based on ordinary personal computers (PCs). To ensure uniform behavior from one machine to the next, each PC should be booted from a diskette containing the operating system, all software and the ballot definition. The software should make the machine invulnerable to rebooting with [Ctrl]+[Alt]+[Del]. There should be some way to prevent anyone from swapping diskettes in the middle of voting. Finally, there should be some simple way for a voting official to enable a single voter to vote once (something analogous to the enabling button on the side of a mechanical lever machine).

All of the desired features listed above were designed and implemented in a functional prototype voting system before classes resumed the first week of January, 2001. The main program was in interpreted QBASIC, and keyboard control was a tiny machine language program. DOS and QBASIC, of course, were included on the diskette. A “Permission Box” with two status-indicating LEDs and one pushbutton was attached to the PC’s serial port. A diskette lock-and-seal system prevented diskette removal without destroying the cable-tie-like seal.

Having *everything* (including final results) on a single diskette gives this system a security feature unmatched by any other voting system: the ability to distribute to opposition parties, news media, security experts, etc.

exact copies of what goes into the voting machine and what comes out of it.

By February of 2001 the BASIC program had been compiled, and a fifth-grade class having a career day focusing on inventions became the first group to test the system publicly. That summer the software was rewritten in C, with assembly language routines for keyboard control and diskette copying. FreeDOS had been developed enough to serve as the operating system, eliminating licensing problems. The Permission Box and diskette seal were redesigned for lower cost. Since then the software has been continually tested and refined, improving security, usability and flexibility. This voting system is called SAVIOC.

### 3. Voting system accuracy

Counting errors of one or two percent and recounts that always come up with different numbers once were considered “normal”. When an election clearly goes one way or the other, a 2% error makes no difference. Even when an election is closer, if most voters see little difference between the candidates, who cares? Now, when there are significant philosophical differences between major candidates and a near-even split in the electorate, the U.S. finally seems to be concluding that such inaccuracies are unacceptable.

Theoretically, a computer-based (DRE) system should be virtually 100% accurate. Computers are binary and have very low failure rates, whereas analog systems involving complex gear trains, card punches, optical sensing or human judgment are known to have significant error rates [14]. Unfortunately, computer-based systems have *not* proven to be 100% accurate [15].

Outright programming errors can produce voting inaccuracies, and may account for some cases where votes were completely lost. These should be rare. On the other hand, a major avenue for inaccuracy in DRE systems exists when the system design stores ballot information in two different forms that can become desynchronized. (The voter sees or hears one thing; the machine records votes as something different.) As one clear example, one class of voting machines uses a paper overlay on a panel of lights and switches. If the positions of the names on the paper do not exactly correspond to the switches associated with those names in the program, errors will occur. Similar desynchronization probably accounts for most of the reports of votes for one candidate being credited to another. Such reports generally include some mention of “programmer error” or other human error that created the desynchronization [16]. SAVIOC offers no opportunity for such human error because it uses a single text file as the source for what the voter sees and what is tallied. It even offers the option of producing printed versions of the ballot directly from that same file.

It can reasonably be claimed that no voting system is more accurate than SAVIOC. In more than three years of public testing (starting 2001 February), in spite of continual software upgrading (through 14 major versions), there has never been a vote lost or misattributed.

### 4. Voting system security

As mentioned above, SAVIOC is unique in being able to make available to the public the exact code used to control the voting machine. When a voting machine is about to be started, multiple diskettes are available. One is selected to boot and define the voting machine; the others are distributed to interested parties. At the end of voting, multiple copies of the final diskette are produced and similarly distributed. This public disclosure can effectively block back-room count manipulations before or after the voting.

Many national politicians, state politicians, computer experts and concerned citizens are clamoring for “voter-verified paper ballots” [17]. Most of those are completely unaware of the SAVIOC concept, and the few that have heard of it tend to dismiss it before even understanding it. The existing software *can* produce those paper records, but so far has done so only on an ordinary computer printer. Because unique printer commands can be added within a ballot file, the process could be adapted to a supermarket-type thermal tape printer without any software changes. Unfortunately, a legal requirement for such paper records actually could *reduce* the security of a SAVIOC system. If the single set of paper records is considered more authoritative than multiple sets of diskette records, then whoever controls the paper can control the election.

The preceding paragraphs cover just the bare bones of SAVIOC’s major security feature, leaving plenty of room for readers to object, “What about ....” A complete discussion of security issues would be a major paper in itself; however, some of the more obvious ones will be addressed briefly in the paragraphs below. Three things should be kept in mind when considering voting security: (1) One of the easiest ways to affect an election now is to buy absentee ballots. (2) If one type of voting system becomes extremely wide-spread, one type of attack could cause major havoc. (3) It does little good to insist on absolute bulletproof security in one part of the entire voting system if other parts provide gaping holes.

Couldn’t hackers interfere with voting as it is going on? No. The computers are not connected to any network.

Couldn’t the diskette used in the computer be different from the ones distributed? Not if the poll watchers are doing their job. The manual that is downloaded with the software gives numerous ways to avoid that risk. Additionally, the diskettes distributed at the end probably would reveal the substitution.

Couldn't someone remove the original diskette at some point and replace it with one that has different totals? No. Even if the physical seal is breached, the software recognizes when the diskette has been removed. The program stops and sounds an alarm.

Couldn't someone replace the proper software with a program that appears to work the same, but can be triggered by a special key combination to distort the results? No. The software on the distributed diskettes can be compared bit-for-bit with that on the master web site [18].

Couldn't someone hack that master web site? Any web site can be hacked, but it can't *stay* hacked. Downloads can be made at any time, and for security reasons should be made at two different times well before the elections. Any difference between the two downloads is a signal that something is wrong. Furthermore, hashing results can be used to check validity (this is not yet implemented), and alerts could be sent to all registered users.

What if nobody bothers to receive the diskettes that are to be distributed? This probably means that those election officials are completely trusted, and there is no security problem at that location.

It can reasonably be claimed that SAVIOC is more secure than any other voting system.

## 5. Voting system trustworthiness

Absolute trustworthiness cannot be proven; it can merely be inferred from a lack of negative data. Negative data can include objective information such as clearly recorded failures, and subjective information such as suspicious anomalies, secrets and questionable behavior, motives or associations [19].

To the best of the author's knowledge, no voting technology can claim zero failures. SAVIOC has never misplaced a vote, but there have been a few times when software bugs resulted in a failure to start or an early shutdown. (All such known bugs have been corrected.) Furthermore, although thousands of voters have cast ballots on SAVIOC, as of this writing only one person other than the author has tried to start up the system as a voting official would.

In the subjective areas, SAVIOC may have significant advantages over most of the leading vendors. There is no "secret" software or hardware [20]. There is no "special" software for any location [21]. (Everyone downloads the same package from the web.) There are no politicians or political fundraisers in control of SAVIOC, as contrasted with some other systems [19]. Because the program is relatively small (about 10,000 lines, versus Diebold's 49,000 lines [22]), a programmer examining it can be far more confident in declaring it free of malicious code.

More extensive testing is necessary, but it is possible that SAVIOC is more trustworthy than any other voting system. It is reasonable to claim that no other system is more trustworthy.

## 6. Voting system usability

Ease of use was an important part of SAVIOC from its inception. Mechanical lever machines, the only voting technology used in the author's county, were considered the antithesis of easy. On such a machine, each row is a political party and each office occupies one or more columns. A lever at each intersection allows picking individual candidates, but a lever at the left of each row permits straight-party votes. In crowded elections, some minor offices may appear lower-down in columns that have other offices at the top. Significantly above this area is a non-party row with a larger text area, used for questions and referenda. Significantly above that is a set of angled slots, corresponding to the office columns at the bottom, where manual write-in votes may be recorded. Short people and people in wheelchairs cannot reach the upper portions of the machine. Even those of average stature easily overlook (underlook?) the questions at the top.

A two-dimensional array can present an obstacle to finding a particular name. Since SAVIOC's ballot is completely linear, a single scan from top to bottom will cover everything. The basic voting interface thus requires only two inputs: "down" and "select". It would have been possible to use those same two inputs at the end of a ballot to signify the choice between "go around again" and "cast my ballot"; however, a third distinct input (the [Y] key, meaning "Yes") was added to avoid any possibility of ending a vote unintentionally. SAVIOC voting (without write-ins) thus can be completed with just three keys: [Y], to start and end voting; [↓] (the down-arrow) to scan down through the ballot; and [Spacebar] to mark a candidate as selected.

Figures 1-4 illustrate the normal cycle each voter would see when voting. These screen captures were done using a "Command Prompt" window in Microsoft Windows 2000 to reduce the saved image size; normally they would be full-screen displays. To capture these screens required running in "Practice Mode", which bypasses security features and allows unlimited voting. The words, "Practice Mode", that appear in the corners on three of the four screens, blink to draw attention to the fact that this is not normal ("real") voting.

Figure 1 represents the screen that shows when between voters. At such times the monitor should be turned toward election officials. The large-format number (visible at a distance) shows how many votes have been cast so far on that machine. Other information useful to voting officials and poll watchers also is displayed here. In real voting, the only way to proceed from this screen is to press the Permission Button.

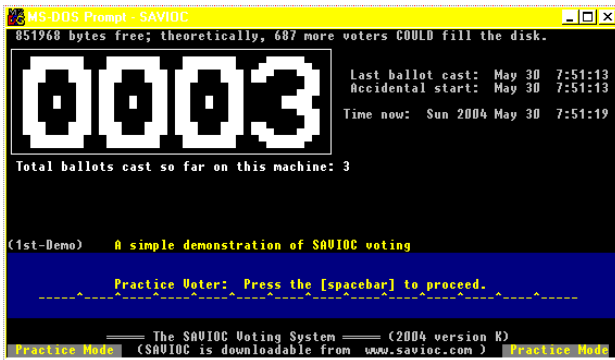


Figure 1. The screen showing between voters. For real voting the text in the blue area would say, “Voter: Ask the voting official to tap the Permission Button.”

Figure 2 shows the screen that appears next for a general election. (A primary requires an intermediate screen to identify the voter’s party.) Once the voter presses the [Y] key, a voting session irrevocably begins.

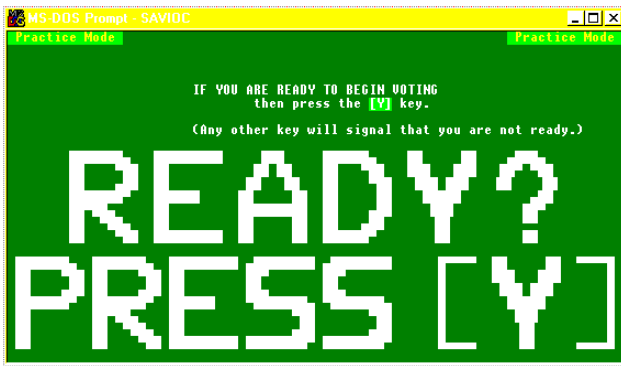


Figure 2. The [Y] key officially starts voting.

Figure 3 shows a representative ballot page. Here, the voter already has moved the cursor beside the desired selection and marked it using the [Spacebar].

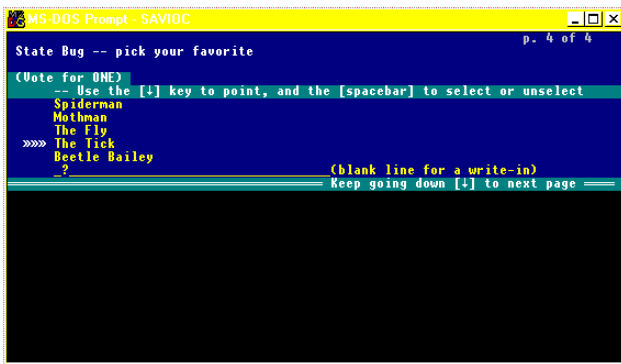


Figure 3. One voting page; one candidate is selected.

Figure 4 shows the final voter screen. Once the voter presses the [Y] key, that voting session irrevocably ends.

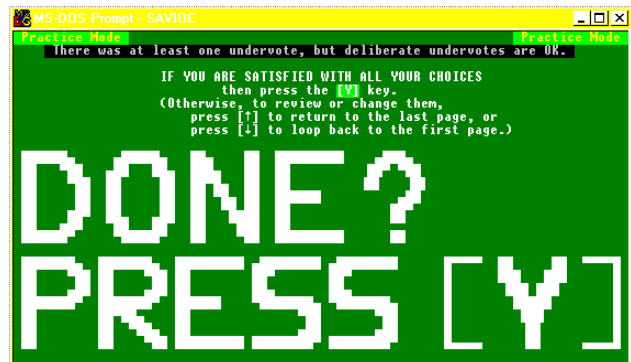


Figure 4. The [Y] key officially ends voting.

Note, in Figure 4, the warning about an undervote. If undervotes exist, there is also an immediately preceding screen (not shown) that gives more explicit and detailed information about them. From either screen the voter can go back to review or change selections, or proceed to the end. Accidental undervotes are possible only if one completely ignores clear warnings. Overvotes are impossible because one is not able to leave a ballot page until enough choices are unselected to eliminate the overvote condition.

Extensive testing has helped eliminate unanticipated user errors. A few examples illustrate this. One person was observed tapping unproductively on the left arrow. The left, right and down arrows now all do the same thing. From the beginning the [Enter] key did the same thing as the [Spacebar] (select or unselect); however, now the [Delete] and [Backspace] keys also function like [Spacebar] because some people tried those keys when they needed to unselect a previous choice. The strangest voter error discovered was when one elderly woman consistently bumped the [Spacebar] as she was reaching for the [Y] key. Maybe no one else would ever have the same problem, but the software was changed to use arrow keys (not in line with the [Y] key) instead of the [Spacebar] to review selections at the end.

SAVIOC has been declared easy to use by both grade school children and senior citizens. Most people with physical disabilities still can hit a few widely-spaced keys on a keyboard. The system even has been used successfully by two people who are legally blind and one who is totally blind. Tones can be requested indicating the current page number and line number, and whether that line is selected. Using those tones, it is possible to vote without seeing the screen, by referring to a copy of the ballot in some other form – Braille, large print, voice on tape, etc.

For one test in a retirement community, helpers were recruited from among the residents. Some of those volunteers literally had never touched a computer before; nevertheless, after one or two ballots they were instructing others. It was a real revelation to overhear one of those helpers say to a friend, "If it were this easy, you wouldn't have to vote straight-party."

There has been no opportunity for the author to use and compare other DRE voting systems, but considering the successes of the young, the old and the disabled, it is reasonable to claim that SAVIOC is eminently usable.

## 7. Voting system cost

Old computers are free. Not only are they being discarded, they are being discarded in quantities that raise environmental concerns [23]. The author's campus has a student group that refurbishes donated machines and gives them to non-profit groups in the area. The space dedicated to this operation is about 335 m<sup>2</sup> (3600 ft<sup>2</sup>). Figure 5 shows just a portion of the system units stacked there. It is noteworthy that anything older than a Pentium II is considered too old to be given away. In contrast, SAVIOC runs fine on a 20 MHz 386 with just 4 Mb of memory and a dead hard drive!

The capital cost of a single SAVIOC voting system probably would be in the vicinity of \$25, for the Permission Box and the diskette lock-seal system – **unless** voter verifiable paper ballots are required. In that case the capital cost jumps by more than a factor of 20. A thermal tape printer with full cutoff costs about \$500, and still needs a large sealed box with a window to display and then catch the ballot records. Those are the only specialized pieces of equipment required for SAVIOC voting. Other DRE systems tend to cost in the thousands per station.



Figure 5. Free computers.

Insurance against power failures could be considered part of the cost, but such equipment is usable elsewhere the rest of the year. An uninterruptible power supply (UPS) can be found for \$40, and another \$100 will get an inverter (to be installed in a nearby vehicle) capable of supplying several computers as well as room lights.

As with other DRE systems, consumables are almost negligible. Even with a modest software license fee added, operating costs for SAVIOC would be less than the consumables cost for the notoriously inexpensive punch card systems [24], and less than just the storage costs for mechanical lever machines [25] (to say nothing of maintenance, repair and transportation costs). Note that no licensing fee is required for mock elections, student elections, union elections or even the election of unpaid school board members; licensing applies only for the election of paid public officials.

It can reasonably be claimed that SAVIOC is less expensive than any other voting system.

## 8. Conclusions

The basic concepts of SAVIOC make it arguably more secure and less expensive than any other voting system in existence. The implementation makes it accurate, trustworthy and very easy to use. Distribution via the web makes it easy to try, test and verify. All that is missing is actual use in an election.

SAVIOC is an acronym for Secure and Accurate Voting on Inexpensive Old Computers.

## 9. References

A few references are merely URLs. In such cases the entire web site (or at least the page directly referenced) applies to the point that is being made where that reference number appears in the text above.

- [1] Richie, Rob (2001 May 9). *Needed: A Commitment to Democracy*. Retrieved 2004 June 1, from the FairVote web site: [http://www.fairvote.org/op\\_ed/knightridder.htm](http://www.fairvote.org/op_ed/knightridder.htm)
- [2] Pettys, Dick (2002 Sept. 17). *Some fear Georgia's new voting machines will be replay of Florida problems*. Retrieved 2004 June 1, from the KioskCom web site: [http://www.kioskcom.com/articles\\_detail.php?id=1530](http://www.kioskcom.com/articles_detail.php?id=1530)
- [3] Dickson, J. (2003 Sept. 24). *Maryland Proceeding with Diebold Voting Machines Contract*. Retrieved 2004 June 1, from American Association of People with Disabilities web site: <http://www.aapd-dc.org/dvpmain/votemachines/dieboldvm.html>
- [4] Shepard, S. (2003 Dec. 6). *Growing Movement Questions Integrity of E-Voting*. The Atlanta Journal-Constitution. Retrieved 2004 May 26, from <http://www.rense.com/general45/growingmovement.htm>

- [5] Landes, L. (2004 April 28). *Two voting companies & two brothers will count 80 percent of U.S. election using both scanners & touchscreens*. Retrieved 2004 May 26, from the Online Journal web site: <http://www.onlinejournal.com/evoting/042804Landes/042804landes.htm>
- [6] Gray, Heather (2004 Feb 12). *Georgia's "Faith-Based" Electronic Voting System: Something's Rotten in the State*. Retrieved 2004 June 1, from the Common Dreams web site: <http://www.commondreams.org/views04/0212-11.htm>
- [7] Wasserman, J. (2004 April 30). *Calif. Official Bans Some Voting Machines*. AP article retrieved 2004 June 1, from the FairElections web site: <http://www.fairelections.us/article.php?id=208>
- [8] Kohno, T., Stubblefield, A., Rubin, A. D., Wallach, D. S. (2003 July 23). *Analysis of an Electronic Voting System*. Retrieved 2004 June 1, from <http://avirubin.com/vote.pdf>
- [9] <http://www.verifiedvoting.org/>
- [10] <http://www.electionreform.org/ERMain/priorities/netvote/default.htm>
- [11] Coleman, K. (2003 Jan. 1). *Internet Voting*. Retrieved 2004 June 1, from the U.S. Dept of State Foreign Press Center web site: <http://fpc.state.gov/documents/organization/22714.pdf>
- [12] Keating, D. (2004 March 31). *Voting, Security Fears Derail \$22 Million Experiment*. The Washington Post, Page A23.
- [13] *Electronic Voting Firm Site Hack*. (2003 Dec. 29). Retrieved 2004 May 31, from the Wired News web site: <http://www.wired.com/news/evote/0,2645,61764,00.html>
- [14] Adams, Brian J. (2001 Feb. 28). *Identification of Voting Machine Errors During the 2000 General Election in Lancaster County, Pennsylvania*. Retrieved 2004 June 1, from the CalTech web site: <http://www.vote.caltech.edu/Reports/adams.pdf>
- [15] Peterson, Kavan (2004 May 3). *Integrity of electronic voting questioned*. Retrieved 2004 June 1, from the StateLine web site: <http://www.stateline.org/stateline/?pa=story&sa=showStoryInfo&id=368968>
- [16] Corral, Oscar (2002 April 4). *Technician's error, not machines, to blame in Dade election*. Retrieved 2004 June 1, from the Miami Herald site: <http://www.miami.com/mld/miamiherald/news/local/2993042.htm>
- [17] *The Computer Ate My Vote* (n.d.). Retrieved 2004 June 1, from the TrueMajority web site: <http://www.truemajority.org/ComputerAteMyVote/index.cfm>
- [18] <http://www.savioc.com>
- [19] Fittrakis, Bob, Wasserman, Harvey (2004 March 5). *Diebold's Political Machine*. Retrieved 2004 June 1, from the Mother Jones web site: [http://www.motherjones.com/commentary/columns/2004/03/03\\_200.html](http://www.motherjones.com/commentary/columns/2004/03/03_200.html)
- [20] *Electronic Voting - Overview and Issues* (2004 May). Retrieved 2004 June 1, from the Berkeley web site: <http://www.igs.berkeley.edu/library/htElectronicVoting2004.html>
- [21] Zetter, Kim (2003 Nov. 6). *Suspect Code Used in State Votes*. Wired News. Retrieved 2004 June 1, from <http://news.lycos.com/news/story.asp?section=MyLycos&storyId=797139>
- [22] Schwartz, John (2004 May 3). *Who Hacked the Voting System? The Teacher*. The New York Times. Retrieved 2004 June 1, from the FairElections web site: <http://www.fairelections.us/article.php?id=211>
- [23] Peterson, Kavan (2003 Oct. 24). *E-waste Disposal -- States' Computer-Age Headache*. Retrieved 2004 June 1, from <http://www.govtech.net/news/news.php?id=74557>
- [24] Cards cost a minimum of \$0.07 per voter per election, according to a vendor of punch cards. Telephone conversation in 2001.
- [25] Lancaster County, PA pays \$48,000 per year to store fewer than 500 voting machines, according to a voting official. Personal communication in 2001.