A PC-Based Open-Source Voting Machine with an Accessible Voter-Verifiable Paper Ballot

Arthur M. Keller, UC Santa Cruz and Open Voting Consortium
ark@soe.ucsc.edu
Alan Dechert, Open Voting Consortium
alan@openvotingconsortium.org
Karl Auerbach, InterWorking Labs
karl@iwl.com
David Mertz, Gnosis Software, Inc.
mertz@gnosis.cx

1. Introduction

The heart of democracy is voting. The heart of voting is trust that each vote is recorded and tallied with accuracy and impartiality.

The Open Voting Consortium (OVC) is creating a trustworthy, cost effective, voter verifiable voting system using open source software components on industry standard computers. A primary element of this Open Voting system is the use of software through which the voter creates a printed paper ballot containing his or her choices. Before casting his or her ballot the voter may use other, independently programmed, computers to validate that the ballot properly reflects the voter's choices. The paper ballot is cast by placing it into a ballot box. Once cast, that paper ballot is the authoritative record of the voter's choices for the election and for any recount of that election. Open Voting ballots are machine-readable and may be tabulated (and verified and re-tabulated in the case of a recount) either by computer or by hand.

Open Voting systems can be engineered to accommodate the special needs of those who have physical impairments, or limited reading ability.

Voting is the foundation of democratic systems, whether those be direct or representative systems. There is no shortage of historical anecdotes of attempts to undermine the integrity of electoral systems. The paper and mechanical systems we use today, although far from perfect, are built upon literally hundreds of years of actual experience.

There is immense pressure to replace our "dated" paper and mechanical systems with computerized systems. There are many reasons why such systems are attractive. These reasons include, cost, speed of voting and tabulation, elimination of ambiguity from things like "hanging chads", and a belated recognition that many of our traditional systems are not well-suited for use by citizens with physical impairments.

Many of us today have come to trust many of our financial transactions to ATM’s (automatic teller machines). The push for electronic voting machines has been a beneficiary of that faith in ATMs. However, we are starting to learn that that faith is unwarranted.

First of all, ATM machines do fail and are often attacked. Those who operate ATM's usually consider the loss rate to be a proprietary secret. Banks are well versed in the actuarial arts and they build into their financial plans various means to cover the losses that do occur. In more crude terms, it's only money.

Voting machines carry a more precious burden - there is no way to buy insurance or to set aside a contingency fund to replace a broken or tampered election.

There are several areas of concern regarding the new generation of computerized voting machines:

- No means for the voter to verify that his/her votes have been tallied properly.
- No means outside of the memories of the voting machines themselves to audit or recount the votes.
- Lack of ability to audit the quality of the software. Fortunately the widespread belief that "computers are always right" is fading. Our individual experiences with error-ridden software on personal computers and consumer products (e.g. the BMW 745i[1]), software errors by even the best-of-the-best (e.g. NASA and the loss of the Mars Climate Orbiter[2]), and the possibility that intentional software bugs can be hidden so deeply as to be virtually invisible (Ken Thompson's famous 1984 paper - Reflections on Trusting Trust[3]) have all combined to teach us that we should not trust software until that trust has been well earned. And even then, we ought not to be surprised if unsuspected flaws arise.
- Vulnerability of the machines or of their supporting infrastructures to intentional attack or inadvertent errors.

The companies that produce voting machines have poured gasoline onto the smoldering embers of concern. Some of these products are built on Microsoft operating systems - operating systems that have a well-earned reputation for being penetrable and insecure. And most of these companies claim that their systems are full of trade secrets and proprietary information and that, as a consequence, their internal workings may not be inspected by the public. In addition, these companies have frequently displayed a degree of disdain (in some cases disdain that takes the form of lawsuits) against those who are concerned about the integrity of these products. And finally, these companies themselves have frequently demonstrated an appalling lack of sophistication regarding the protection of their systems, procedures, and corporate computer systems. There is a widespread perception that these companies are more concerned about profits than about fair and trustworthy elections.

The Help America Vote Act of 2002[4] was passed into law to modernize voting equipment as a result of the 2000 US Presidential election and the problems observed in Florida.[5] The Federal Election Commission (FEC) has issued a set of Voting System Standards (VSS)[6] that serve as a model of functional requirements that elections systems must meet before they can be certified for use in an election. The next section discusses the existing voting machines that meet those standards. Section 3 considers the rationale for an accessible voter-verifiable paper ballot. Section 4 is a description of the Open Voting Consortium architecture for the polling place. Section 5 mentions the current state and next steps. Conclusion, acknowledgements, and references follow.

2. Existing Electronic Voting Machines

Existing DRE (Direct Recording Electronic) voting machines have come under increasing scrutiny.

2.1 Diebold AccuVote TS and TS-X

A group led by Avi Rubin analyzed the Diebold AccuVote TS DRE voting machine and found numerous flaws.[7] SAIC was commissions by the state of Maryland to do another analysis of the Diebold voting system and found "[t]he system, as implemented in policy, procedure, and technology, is at high risk of compromise."[8] Based on these reports, the California Secretary of States office established security procedures for DRE voting machines.[9] Diebold used uncertified software in their electronic voting equipment in California.[10] Diebold was then banned from California elections by the California Secretary of State.[11]

2.2 Other DRE Voting Machines

Other DRE vendors are proposing to add printers to their DREs.[12] AccuPoll has an Electronic Voting System with a voter-verified paper audit trail.[13] Sequoia Voting Systems is marketing optional voter verifiable paper record printers for their DREs.[14] The state of Nevada will use these VeriVote printers in the 2004 election.[15] The Avante VOTE-TRAKKER is a DRE with a voter-verifiable paper audit trail.[16]

3. Why an Accessible Voter-Verifiable Paper Ballot

Many computer and other experts have joined VerifiedVoting.org's call for "the use of voter-verified paper ballots (VVPBs) for all elections in the United States, so voters can inspect individual permanent records of their ballots before they are cast and so meaningful recounts may be conducted. We also insist that electronic voting equipment and software be open to public scrutiny and that random, surprise recounts be conducted on a regular basis to audit election equipment."[17]

3.1 Paper Receipts vs. Paper Ballots

We speak of OVC creating a paper *ballot*, not a receipt, nor simply a "paper trail." That is, for OVC machines, the printout from a voting station is the primary and official record of votes cast by a voter. Electronic records may be used for generating preliminary results more rapidly, but the paper ballot is the actual official vote document counted.

Some writers discuss producing a paper receipt, which a voter might carry home with them, as they do an ATM receipt. There are two significant problems with this approach. In the first place, if we suppose that a voting station might have been tampered with and/or simply contain a programming error, it is not a great jump to imagine that it may print out a record that differs from what it records electronically. A receipt is a "feel good" approach that fails to correct the underlying flaws of DREs.

But the second problem with receipts is even more fundamental. A voting receipt that can be carried away by a voter enables vote buying and vote coercion. An interested third party—even someone as seemingly innocuous as an overbearing family member—could demand to see a receipt for voting in a manner desired. With OVC systems, ballots must be placed into a sealed ballot box to count as votes. If a voter leaves with an uncast ballot, even if she went through the motions of printing it at a vote station, that simply does not represent a vote that may be "proven" to a third party.

What some vendors refer to as a paper trail suffers from a weakness similar to the first problem paper receipts suffer. Under some such models, a DRE voting station might print out a summary of votes cast at the end of the day (or at some other interval). But such a printout is also just a "feel good" measure. If a machine software or hardware can be flawed out of malice or error, it can very well print a tally that fails to accurately reflect the votes cast on it. It is not *paper* that is crucial, but *voter-verifiability*.

3.2 Paper Audit Trail Under Glass vs. Paper Ballot.

While "ballot under glass" does indeed do a pretty good job of preventing ballot box stuffing with forged physical ballots, this approach is not the only—nor even the best—technique to accomplish this goal. We plan for OVC systems to incorporate cryptographic signatures and precinct-level customization of ballots that can convincingly prove a ballot is produced on authorized machines, at the voting place, rather than forged elsewhere. A simple customization of ballots is a variation of the page position of our ballot watermarks in a manner that a tamperer cannot produce in advance. Surprisingly much information can be subtly coded by moving two background images a few millimeters in various directions. Another option is to encode a cryptographic signature within the barcode on a ballot—in a manner that can be mathematically proven not to disclose anything about the individual voter who cast that vote, but simultaneously that cannot be forged without knowledge of a secret key.

There are several narrowly technical problems with "ballot under glass" systems. For one thing, such a system will almost inevitably be more expensive than one that can use commodity printers and paper stock, such as OVC’s solution. But voting is too important to be decided on cost, so that is an incidental issue. Along a similar line, a "ballot under glass" system has some extra mechanical problems with allowing rejection of incorrect ballots; some sort of mechanism for sending a spoiled ballot somewhere other than to the ballot-box is needed. Again, this adds cost and more points of physical failure.

A more significant issue for "ballot under glass" systems is their failure to provide the quality of accessibility to vision- or reading-impaired voters that OVC's design does. Ordinary sighted voters who happen to need reading glasses are likely to find "ballot under glass" systems more difficult to check than are OVC printed ballots. Even if these machines add provisions for audio feedback on final ballots, users are dependent on the very same machine to provide such audio feedback. Potentially, a tampered-with machine could bias votes, but only for blind voters (still perhaps enough to change close elections). In contrast, OVC positively encourages third parties to develop software to assure the barcode encoding of votes matches the visibly printed votes—every voter is treated equally, and all can verify ballots.

From a more sophisticated cryptology perspective, "ballot under glass" systems are likely to compromise voter anonymity in subtle ways. One of the issues the world-class security researchers with OVC have considered is the possibility that sequential or time-stamp information on ballots could be correlated with the activity of individual voters. Even covert videotaping of the order in which voters enter a polling place might be used for such a compromise. This is just part of the threat analysis study that we plan to perform in order to create a reliable, secure, and trustworthy election system.

3.3 Accessible Voting

One of the key benefits of Electronic Voting Machines is to allow disabled voters to vote unassisted. [18] However, as the movement for a voter-verifiable paper audit trail grows,[19] there is a need for the paper audit trail to be accessible as well.[20] The Open Voting Consortium's voting system is designed to be accessible for both entering the votes and verifying the paper ballot produced.

4. OVC System Overview

The Open Voting Consortium (OVC) is developing a PC-based open source voting machine with an accessible voter-verified paper ballot. The polling place system consists of a Voter Sign-in Station, an Electronic Voting Machine, an Electronic Voting Machine with a Reading Impaired Interface, a Ballot Verification Station, and a Ballot Reconciliation Station. In addition, there are components at the county canvassing site that are discussed only briefly in this paper.

4.1 Voter Sign-in Station

The Voter Sign-In Station is used by the poll worker when the voter signs in and involves giving the voter a "token." It is a requirement that each voter cast only one vote and that the vote cast be of the right precinct and party for the voter. The "token" authorizes the voter to cast a ballot using one of these techniques.

- Pre-printed ballot stock
    - Option for scanning ballot type by EVM
- Poll worker activation
- Per-voter PIN (including party/precinct identifier)
- Per-party/precinct token
- Smart cards

The token is then used by the Electronic Voting Machine and the Electronic Voting Machine with the Reading Impaired Interface to ensure that each voter votes only once and only using the correct ballot type.

If the voter spoils a ballot, the ballot is marked spoiled and kept for reconciliation at the Ballot Reconciliation Station, and the voter is given a new token for voting.

4.2 Electronic Voting Machine

The Electronic Voting Machine consists of these components:

- A PC, preferably stock commodity hardware, with these features:
    - A monitor, preferably LCD, possibly 17" touch-screen measured diagonally.
    - One or more input devices, such as:
        - Touch-screen interface on LCD screen
        - Mouse
        - Keyboard
        - Buttons surrounding the screen, like on an ATM
        - Numeric keypad
        - Symbolic keypad
    - Possibly a smart card reader/writer
- A CD-R drive. The CD-R will contain:

    - The operating system, e.g., a stripped down Linux distribution
    - The EVM software
    - Ballot Definition files and public keys of various external components
    - Optionally, sound files for the ballot (included for the Electronic Voting Machine with the Reading Impaired Interface)
    - Personalization, potentially including public/private key pairs for this voting machine
    - Startup record, possibly including generated public key of this voting machine
    - Electronic Ballot Images (EBIs), in XML format (and possibly in Postscript format), written at end of day in ascending order by (randomly generated) ballot ID
    - The CD-R is used subsequently by the Ballot Reconciliation System and possibly during county canvassing.
- A printer with these specifications:
    - Inkjet or laser
    - Preferably output page is obscured from view (either by appearing face down, or by a cover)
    - Unprintable margin of no more than 7.5mm on all sides
    - Feedback to the user (auditory or visual) that the ballot is printing and will come out soon
    - Prints a test document at the start of a voting day that includes records of the public keys for the EVM for this day.
    - Potentially takes blank ballot stock given to voter upon sign-in. Otherwise, includes storage for blank ballot stock for printing. Blank ballot stock may be specially printed paper, possibly pre-printed on reverse side (with "please turn over" message).
    - Prints ballot in printed ballot format potentially using special printed ballot stock.
    - The ballot can be read by the Ballot Verification Station and includes text in OCR format, plus a barcode for more foolproof reading.
- A persistent EBI storage device, such as a USB memory dongle (i.e., a USB flash memory device) for persistently storing the EBIs until the end of the day, when the EBIs are transferred onto the CD-R. The USB memory dongle is kept for audit purposes.
    - Device should be large enough not to be easily lost
    - Device should be lockable and tamper proof when locked
    - Potentially, device could lock in the open position onto cabinet and PC and lock in the closed position sealed and ready for removal. Device could be set to be open only once, and on subsequent openings the device would be read only.
    - Potentially, with hardware private key for digitally signing the ballot.
- Security enclosure that prevents tinkering with the device

4.3 Electronic Voting Machine with Reading Impaired Interface

The Electronic Voting Machine with Reading Impaired Interface is a PC similar to the Electronic Voting Machine described above that includes auditory output of the ballot choices and selections made and also includes additional modes of making selections suitable for the blind or reading impaired. Whether these features are integrated to a common voting machine with all functionality, or whether there is a separate configuration for the disabled, is an open question.

For example, additional modes of input may be useful for those who can read printed materials, but have physical limitations. The idea is for a universal design that accommodates all voters.

The electronic voting machine for the reading impaired produces a printed ballot that can be processed by the Ballot Verification Station.

4.4 Ballot Verification Station

The Ballot Verification Station reads the ballot produced by the Electronic Voting Machine or the Electronic Voting Machine with Reading Impaired Interface and speaks (auditorily) the selections on the voter's ballot. A count is kept of usage, including counts of consecutive usage for the same ballot, but no permanent record is kept of which ballots are verified.

The PC boots off the CD-R, which includes the following:

- The operating system
- The BVS software
- Ballot Definition files and public keys of various Electronic Voting Machines
- Sound files for the ballot
- Personalization
- Startup record
- Non-ballot identifying statistics on usage

It is possible for the Ballot Verification Station to have a screen and to display the selections on the screen at the voter's option. Such an option (enabled by the voter upon her request) would enable a voter who can read to verify that her ballot will be read correctly for automated tallying.

4.5 Ballot Reconciliation Station

The Ballot Reconciliation Station reads the paper ballots and reconciles them against the Electronic Ballot Images (EBIs) on the CD-Rs from the Electronic Voting Machine or the Electronic Voting Machine with Reading Impaired Interface.

The Ballot Reconciliation Station includes the following components:

- Scanner, preferably page fed
- PC
- Monitor
- Input devices: keyboard, mouse
- Printer
    - Prints vote totals for posting
- CD-R
    - Like the other CD-R; includes cumulative copy of EBIs as well as vote totals by precinct.

The Ballot Reconciliation System runs the Ballot Reconciliation Procedure, which is beyond the scope of this paper.

4.6 Paper Ballot

The paper ballot is generated by the Electronic Voting Machine or the Electronic Voting Machine with Reading Impaired Interface. It is the paper on which the voter’s choices are recorded. It must be “cast” in order to be tallied during canvassing, testing, or a manual recount.

The paper ballot is intended to be easily read by the voter so that the voter may verify that his or her choices have been properly marked. It also contains security markings and a bar code. The bar code encodes the user’s choices, as expressed in the human readable portion of the ballot. The human readable text should be in an OCR-friendly font so it is computer-readable as well. The voter may use the Ballot Verification Station to verify that the bar code accurately reflects their choices. The Ballot Verification Station not only assists sight-impaired and reading-impaired voters in verifying their ballots, but also to give any voter the assurance that the bar-code on the ballot properly mirrors their choices, as represented in the human-readable text on the ballot.

The bar code consists of several things:

- Identifiers, such as the date, election, precinct, type of ballot, polling machine, and random ballot ID for reconciliation against the electronic record made by the Electronic Voting Machine or the Electronic Voting Machine with Reading Impaired Interface.
- The selections made by the voter.
- Checksums to detect processing errors.
- Additional padding data to obscure the bar code so that poll workers, who will be able to see the bar code (but not the textual part of the ballot) will not be readily able to ascertain by eye what selections the voter made.
- The bar code is designed so that none of the information in the bar code can be used to identify any voter personally.

Spoiled paper ballots are kept by the Ballot Reconciliation System to be reconciled against Electronic Ballot Images (EBIs) produced by the Electronic Voting Machine or the Electronic Voting Machine with Reading Impaired Interface.

4.7 Privacy Folder

The paper ballot contains the voter’s choices in two forms: a form that can be read by people and a bar code that expresses those choices in a machine readable form.

Poll workers may come in contact with the ballot should they be asked to assist a voter or to cast the ballot into the ballot box. In order to protect voter privacy it is desirable to minimize the chance that a voting place worker might observe the voter's ballot choices.

A privacy folder is just a standard file folder with an edge trimmed back so that it reveals only the bar code part of a ballot. The voter is expected to take his/her ballot from the printer of the Electronic Voting Machine or the Electronic Voting Machine with Reading Impaired Interface and place it into a privacy folder before leaving the voting booth.

The privacy folder is designed so that the voter may place the ballot still in its folder against the scanning station of Ballot Verification Station to hear the voter's ballot's choices spoken.

When handed the ballot by the voter, the poll worker casts the ballot by turning the privacy folder so the ballot is face down, and then sliding the paper ballot into the ballot box.

4.8 Ballot Box

This is a physically secure container, into which voters have their paper ballots placed, in order to "cast" their votes. The mechanical aspects of the voting box will vary from jurisdiction to jurisdiction, depending on local laws and customs.

4.9 Box for Spoiled Ballots

When a voter spoils a ballot, perhaps because the ballot does not accurately reflect her preferences, the ballot is marked spoiled and placed in a box for spoiled ballots for later reconciliation.

5. Current Status and Next Steps

A demonstration system was shown at the Santa Clara County Government Building in San Jose, California on April 1, 2004. This demonstration was featured on KGO-TV and KCBS and KGO radio later that day and described in the San Jose Mercury News that morning.[21] On April 8, 2004, the San Jose Mercury News referred to our system in an editorial as a "Touch Screen Holy Grail."[22] Further demonstrations were given at the Computers, Freedom, and Privacy conference in Berkeley, California on April 23, 2004.[23] Another demonstration was given at the PlaNetwork conference in San Francisco, California on June 6, 2004.[24]

Several state colleges and the Open Voting Consortium are currently in discussions with their respective Secretaries of States to obtain HAVA funding to build production-quality reference versions of this system.

6. Conclusions

The Open Voting Consortium has demonstrated a voting system based on a PC-based electronic voting machine with voter-verifiable accessible paper ballot. We have described the design for the production system we propose to build, based on the prototype we have built and the lessons learned in the process. In the development of this system, we expect to enhance the state of the art in building reliable and trustworthy computerized systems. However, it is not merely the software and hardware components that are of concern; the voting processes and procedures are also key to the development of a reliable, secure, trustworthy and accessible system.

7. Acknowledgements.

We acknowledge the efforts of the volunteers of the Open Voting Consortium who contributed to the design we describe. In particular, Alan Dechert developed much of the design and Doug Jones provided significant insights into voting issues. The demonstration software was largely developed by Jan Kärrman, John-Paul Gignac, Anand Pillai, Eron Lloyd, David Mertz, Laird Popkin, and Fred McLain. Karl Auerbach wrote an FAQ on which parts of this paper is based. Amy Pearl also contributed to the system description. Joseph Lorenzo Hall contributed useful background.

Our work was inspired by Curtis Gans, Roy Saltman, Henry Brady, Ronnie Dugger, Irwin Mann, and others who have spoken out on the need for auditable, consistent, secure and open election administration. In the last two years, David Dill and Bev Harris have been especially helpful. David Dill referred several people to the OVC, and he and Bev Harris have helped the public recognize the need for a voter-verified paper audit trail.

8. References.

[1] Dorian Miller, “BMW 745 Bug,” September 22, 2002, found at http://www.cs.unc.edu/~dorianm/academics/comp290test/bmw745bug.html

[2] Greg Clark, Staff Writer and Alex Canizares, “Navigation Team Was Unfamiliar with Mars Climate Orbiter,” posted November 10, 1999, found at http://www.space.com/news/mco_report-b_991110.html

[3] Ken Thompson, “Reflections on Trusting Trust,” *Communication of the ACM*, Vol. 27, No. 8, August 1984, pp. 761-763, found online at http://www.acm.org/classics/sep95/.

[4] The Help America Vote Act of 2002 (HAVA). 42 U.S.C.A. §§ 15301 - 15545 (West 2004). See http://fecweb1.fec.gov/hava/hava.htm

[5] Lorrie Faith Cranor, “Voting After Florida: No Easy Answers,” March 19, 2001, available from http://lorrie.cranor.org/voting/essay.html

[6] Federal Election Commission, Voting System Standards, Vols. 1 & 2 (2002), available at http://www.fec.gov/pages/vssfinal/ (Microsoft DOC format) or http://sims.berkeley.edu/~jhall/fec_vss_2002_pdf/ (Adobe PDF format).

[7] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, *Analysis of an Electronic Voting System*, Proc. IEEE Symposium on Security and Privacy (May, 2004), found at http://avirubin.com/vote/analysis/index.html

[8] http://www.dbm.maryland.gov/dbm_search/technology/toc_voting_system_report/votingsystemreportfinal.pdf

[9] See http://www.ss.ca.gov/elections/ks_dre_papers/ks_ts_press_release.pdf

[10] See http://www.wired.com/news/evote/0,2645,61637,00.html?tw=wn_tophead_2

[11] See http://www.ss.ca.gov/executive/press_releases/2004/04_030.pdf

[12] See http://www.wired.com/news/business/0,1367,58738,00.html

[13] See http://www.accupoll.com/News/PressReleases/2003-10-10.html

[14] See http://www.sequoiavote.com/mediadetail.php?id=74

[15] See http://www.wired.com/news/evote/0,2645,63618-2,00.html?tw=wn_story_page_next1

[16] See http://www.aitechnology.com/votetrakker2/evc308.html

[17] See http://www.verifiedvoting.org/

[18] See http://www.accessiblesociety.org/topics/voting/electionreformlegis.html

[19] See http://www.verifiedvoting.org/

[20] See http://www.ss.ca.gov/elections/ks_dre_papers/avvpat_standards_6_15_04.pdf and http://www.ss.ca.gov/elections/ks_dre_papers/press_release_avvpat_06_15_04.pdf

[21] See http://www.siliconvalley.com/mld/siliconvalley/8328014.htm

[22] See http://www.kentucky.com/mld/mercurynews/news/opinion/8383100.htm

[23] See http://cfp2004.org/program/#votingmachinedemo

[24] See http://www.planetwork.net/2004conf/program.html