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
Amy Pearl, Software Innovations
amy@swinvent.com
Joseph Lorenzo Hall, UC Berkeley SIMS
jhall@sims.berkeley.edu

1. Introduction

Voting is the foundation of a democratic system of government, whether the system uses direct or representative governance. The heart of voting is trust that each vote is recorded and tallied with accuracy and impartiality. 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.

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 verify that the ballot properly reflects the voter's choices. The voter may also visually inspect the text printed on the paper ballot. 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 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.

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 or 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.[4] 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[5] was passed into law to modernize voting equipment as a result of the 2000 US Presidential election and the problems observed in Florida.[6] The Federal Election Commission (FEC) has issued a set of Voting System Standards (VSS)[7] 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. OVC System Description

The OVC system will be very much like a traditional system in which the voter enters the polling place, marks his or her choices onto a paper ballot, and inserts the ballot into a ballot box. Our design applies computer technology to that traditional system. However, unlike some of the other computerized voting systems that change the basic nature of the traditional system, our design applies computer technology only in a limited and conservative way.

The OVC design preserves the paper ballot. However, under the OVC design the voter marks the ballot using a computerized voting station rather than a pencil or colored marker. The ballot is printed in plain text that the voter can read. Voters have the opportunity to inspect the ballot to ensure that it properly reflects their choices.

The OVC design will preserve the ballot box. Voters must insert their paper ballots into the ballot box. The OVC ballots will contain a bar code in addition to the plain text. This bar code makes it easy for the poll workers to count the ballots[8] when the ballot box is opened.

The IVC design will be a voter-verified voting system. The core difference between this and other systems, such as DRE equipped with printers, is that in the OVC design the paper ballot is the actual ballot; information that might be recorded in computer memories or on computer media is used only for security, error-detection, fraud detection/prevention, and auditing.

3. Existing Electronic Voting Machines

Existing DRE (Direct Recording Electronic) voting machines have come under increasing scrutiny with widespread reports of malfunctions, omissions and user interface problems during elections.

3.1 Diebold AccuVote TS and TS-X

A group led by Avi Rubin and Dan Wallach analyzed the Diebold AccuVote TS DRE voting machine and found numerous flaws.[9] SAIC was commissioned by the state of Maryland to analyze the Diebold voting system and found "[t]he system, as implemented in policy, procedure, and technology, is at high risk of compromise."[10] Based on these reports, the California Secretary of States office established security procedures for DRE voting machines.[11] Diebold was then found to have used uncertified software in 17 counties in California.[12] The California Secretary of State then decertified the Diebold and all other DREs on April 30, 2004.[13]

3.2 Electronic Systems and Software iVotronic

ES&S iVotronic is a poll-worker-activated, multilingual touch screen system that records votes on internal flash memory. A poll worker uses a cartridge-like device called a Personal Electronic Ballot (PEB) to turn the machine on and enable voting. Voters first choose their ballot language and then make their selections via a touch screen. When the polls close, poll workers read summary data from each machine onto the PEB via infrared. The PEBs are then transported to election headquarters or their contents transmitted via a computer network.

In September 2002 in Florida, a spot check of machines revealed several precincts with hundreds of voters had one or even no votes cast on Election Day and vote totals produced by the main and backup system did not agree.[14] In October 2002 in Texas, several people reported that their votes registered for a different candidate on screen and, in fact, some votes cast for Republicans were counted for Democrats.[15]

In November 2002, two early-voting locations in Wake County, North Carolina (Raleigh) failed to record 436 ballots due to a problem in the iVotronics' firmware.[16]

3.3 Hart InterCivic eSlate

Hart's eSlate is a voter-activated multilingual voting system where the voter turns a selector wheel and set of buttons to indicate their votes. The eSlate terminals are connected via daisy-chained serial cable to a central controller, the Judges' Booth Controller (JBC), which provides power, vote activation, and vote storage for up to twelve eSlate terminals. A poll worker issues a 4-digit PIN to the voter using the JBC. The voter enters this PIN on an eSlate and votes using its selector wheel and buttons. Once the vote is cast, the vote is transmitted via a cable to the JBC and stored in flash memory on the JBC's Mobile Ballot Box (MBB). The MBB is then either physically transported to election headquarters or its contents transmitted via computer network.

In November 2003, poll workers in Harris County, Texas, confused by the system's complexity, could not get the machines to work properly and had been assigning the wrong ballots to voters using the JBC.[17] In February 2004 in Virginia, voters had to cast paper ballots when the JBC used at one precinct "fried," rendering all the eSlate machines unusable.[18] In March 2004 in Orange County, California, hundreds of voters were turned away when one eSlate machine broke down.[19] At the same time in California, poll workers incorrectly assigned ballots from different precincts to their voters and approximately 7000 voters cast ballots for the incorrect precinct.[20]

3.4 Sequoia Voting Systems AVC Edge

The Sequoia AVC Edge is a voter-activated multilingual touch screen system that records votes on flash memory. Its operation is very similar to the Diebold AccuVote-TS described above.

In March 2002 in Palm Beach County, Florida, the Edge machines froze up when voters selected their ballot language and other reports indicate votes counted for the wrong candidate.[21] As well, 15 PCMCIA cards were temporarily lost and the central system would not report the results and in a very close race many ballots were blank.[22] In April 2002, in Hillsborough County, Florida, one precinct could not transfer data on 24 out of 26 PCMCIA cards; results were faxed and entered in by hand.[23] In March 2003, a similar problem plagued PCMCIA cards.[24] In November 2002, in Bernalillo County, New Mexico, 48,000 people voted early, but no race showed more than 36,000 votes due to a software bug.[25] In June 2004, in Morris County New Jersey, the central tabulation system read only zeros from the PCMCIA cards.[26]

3.5 Other DRE Voting Machines

Other DRE vendors are proposing to add printers to their DREs.[27] AccuPoll has an Electronic Voting System with a voter-verified paper audit trail[28] and Sequoia Voting Systems is marketing optional voter-verified paper record printers for their DREs.[29] The state of Nevada will use these VeriVote printers in the 2004 presidential election.[30] The Avante Vote-Trakker is a DRE with a voter-verified paper audit trail.[31] However, none of these systems are in wide use, and some have not even been certified. None of them meet the current California AVVPAT standards. It will be interesting to see how well the systems in Nevada work during the presidential election in Fall 2004.

3.6 Paper Ballots with Optical Scan Machines

There are several problems with the use of paper ballots that are optically scanned with mark/sense-type tabulation systems. The paper ballot is not accessible to the visually impaired or reading impaired. And the paper ballot must be available in multiple languages as required by the jurisdiction. The use of paper does enable recounts, but potentially suffers from the problems of overvotes, undervotes, and improper changes to ballots (including extraneous marks, which would void the ballot).

3.6.1 AutoMark and Populex

The AutoMark[32] and Populex[35] systems address accessibility problems by using an interface comparable to a Direct Recording Electronic voting machine. Similarly, they can provide support for multiple languages and limit overvotes and undervotes. However, there is the question of whether the printed ballots still have to be in each required language, so that a non-English-speaking voter can still verify his or her ballot. A key benefit of these systems is that the same tabulation system can be used for ballots cast in polling places, absentee ballots, and provisional ballots. But they neither maintain an electronic audit trail nor use digital signatures to detect ballot stuffing.

3.6.2 DREs used internationally

Various countries around the world have chosen to use DRE systems. The Dutch-based NEDAP[36] system is used in the Netherlands, France, Germany, the United Kingdom and Ireland but has been criticized for its flaws.[37] The voting machine developed and used recently in India[38] is very simple and lacks features like disabled and multilingual access. Venezuela chose VVPAT-enabled Smartmatic[39] DREs on which to conduct its recent referendum; it appeared to go smoothly.[40]

4. 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."[41]

4.1 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*.

4.2 Paper Audit Trail Under Glass vs. Paper Ballot

While "paper audit trail 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 polling place, rather than forged elsewhere. For example, 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, which is known only to that electronic voting machine.

There are several narrowly technical problems with "paper audit trail under glass" systems. A "paper audit trail under glass" system has some extra mechanical problems with allowing rejection of incorrect paper record; some sort of mechanism for identifying the paper record as spoiled, perhaps through an ink mark. This approach increases the potential of physical failure, such as paper jams.

A more significant issue for "paper audit trail under glass" systems is their failure to provide the quality of accessibility to vision- or reading-impaired voters that OVC's design does. Sighted voters who happen to need reading glasses, or who can read only large print or closely held print, are likely to find “paper audit trail under glass” systems more difficult to check than printed ballots they can physically hold. 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, “paper audit trail under glass” systems are likely to compromise voter anonymity in subtle ways. One of the issues the world-class security researchers associated with our design 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 problem is more serious in those systems in which the voter-verified paper audit trail is maintained on a continuous paper tape fed onto a take-up spool. However, on systems that cut the audit trail into pieces, one for each voter, that ballots that fell to the bottom of the glass bin may be visible to subsequent voters. Such potential visibility also compromises anonymity. This analysis is just part of the threat analysis study that we will perform in order to create a reliable, secure, and trustworthy election system.

A far more serious problem with a voter-verified paper audit trail is the difficulty of automated tabulation of the audit trail. This problem is especially acute when the voter-verified paper audit trail is cut into pieces, one for each voter. The glass bin is likely to be a mass of coiled paper strips. While the continuous spool approach to the paper audit trail is neater, it suffers from an anonymity problem as identified above. When the paper audit trail can only be used in a manual tabulation process, there will be enormous pressure to minimize its use, thereby reducing its effectiveness. In contrast, the OVC design facilitates automated tabulation of the paper ballots while enabling manual counting and voter-verification also.

4.3 Accessible Voting

One of the key benefits of Electronic Voting Machines is to allow disabled voters to vote unassisted. [42] However, as the movement for a voter-verifiable paper audit trail grows,[43] there is a need for the paper audit trail to be accessible as well.[44] The Open Voting Consortium’s voting system is designed to be accessible for both entering the votes and verifying the paper ballot produced.

5. OVC System Overview

The Open Voting Consortium (OVC) is developing a PC-based open source voting machine with an accessible voter-verified paper ballot. We intend to use an open source operating system for the PC, such as Knoppix, a variant of Linux that boots off of a CD. The polling place system consists of a Voter Sign-in Station, an Electronic Voting Station, an Electronic Voting Station 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.

5.1 Precinct/Polling Place Element

The OVC Precinct/Polling Place Element is intended to provide all of the systems and procedures required for a polling place except for voter rolls, sign-in books and the like. The OVC system will be flexible so that it will be adaptable to applicable laws as well as local preferences.

The OVC design will accommodate polling places in which different classes of voters, for example voters of different parties, may be accommodated with ballots appropriate for that particular voter.

Overall design and operation of the OVC system is simplified because the paper ballot produced by it will be the legal ballot. For example, in the OVC design equipment failures will not be handled at the polling place except to the extent necessary to disconnect the failed unit, seal it, and deploy a backup unit.

The OVC design is very concerned that voters with physical disabilities and limited reading ability are accommodated. It is anticipated that the OVC design will contain variations of the Voting Station and Ballot Verification Station that will be designed with user interfaces tailored to the needs of voters with certain types of physical impairments.

The OVC design will not require substantial changes to the workflow of a typical polling place; voters and poll workers will find that procedures are comparable to those used in existing American polling places.

5.1.1 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 Station and the Electronic Voting Station 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.

5.1.2 Electronic Voting Station

The Voting Station is the voter's primary point of contact with the OVC system. After the voter signs-in, a poll worker will direct the voter to a Voting Station.

The physical appearance of the voting station will be that of a lightweight booth with privacy curtains or walls. There will be an integrated device—an Electronic Voting Station—containing computer, printer, battery, and flat screen display. The display will allow touch-screen use and will be mounted so that it may be adapted for use by voters who stand and voters who are in wheel chairs.

The Voting Station will be designed so that setup and teardown are easy; it is anticipated that installation will be largely an unfold-and-plug-in operation.

The Voting Station will be tamperproof and be engineered to endure physical abuse during shipping, deployment, and use. The Voting Station will be designed so that it may be sealed against unauthorized access with locks and lead/wire seals.

The Electronic Voting Station consists of these components:

- A computer, preferably stock commodity hardware, with these features:
  - A monitor, preferably LCD, possibly 15" or 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 Linux system without unnecessary components
  - The EVM software
  - Ballot Definition files and public keys of various external components
  - Optionally, sound files for the ballot (included for the Electronic Voting Station with the Reading Impaired Interface)
  - Personalization, potentially including public/private key pairs for this voting station
  - Startup record, possibly including generated public key of this voting station
  - 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

5.1.3 Electronic Voting Station with Reading Impaired Interface

The Electronic Voting Station with Reading Impaired Interface is a computer similar to the Electronic Voting Station 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 ideal is a universal design that accommodates all voters.

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

5.1.4 Ballot Verification Station

The Ballot Verification Station reads the ballot produced by the Electronic Voting Station or the Electronic Voting Station 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 computer 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 Stations
- 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.

5.1.5 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 Station or the Electronic Voting Station 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.
- CD drive (not writeable)
    - For loading the CD-R's from the Voting Stations.

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

5.1.6 Paper Ballot

The paper ballot is generated by the Electronic Voting Station or the Electronic Voting Station 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 (but *not* time), election, precinct, type of ballot, polling machine, and random ballot ID for reconciliation against the electronic record made by the Electronic Voting Station or the Electronic Voting Station with Reading Impaired Interface. No information that can identify the voter is included on the ballot.
- 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 Station or the Electronic Voting Station with Reading Impaired Interface.

5.1.7 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 poll 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 Station or the Electronic Voting Station 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.

5.1.8 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.

5.1.9 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.

5.1.10 Box for Provisional Ballots

When a voter shows up at a polling place and does not appear on the voting roll or the voting roll shows that the voter was sent an absentee ballot, then the voter is allowed to vote by being given a "token" for a provisional ballot. A distinctive smart card or a provisional "blank" ballot or even a distinctive privacy folder is given to the voter. When the voter has printed the provisional ballot and hands it to the poll worker, the poll worker seals the provisional ballot in an envelope along with the details necessary to determine whether the ballot should be counted and places the provisional ballot in a box for provisional ballots for later reconciliation.

5.2 Absentee Ballots and Manual Polling-Place Ballots

Paper optical-scan ballots will be used for absentee ballots and also for the manually cast polling-place ballots.

5.2.1 Format and Marking

The format and marking of the absentee ballots will be similar to those of existing optical scan ballot systems.

5.2.2 Acceptance at Polling Place

When an absentee ballot is received at a polling place, a poll worker checks the identification of the person delivering it, places on the envelope a sticker from the absentee ballot audit sheet, and places it in the absentee ballot box.

Manual polling-place ballots are placed in the manual ballot box.

5.2.3 Acceptance by Mail or In-Person at County

When an absentee ballot is received by mail, a county poll worker places on the envelope a sticker from the absentee ballot audit sheet, and places it in the absentee ballot box. When an absentee ballot is hand delivered at the county canvassing site, a county poll worker checks the identification of the person delivering it, places on the envelope a sticker from the absentee ballot audit sheet, and places it in the absentee ballot box.

5.2.4 Validation

The process for validating absentee ballots is comparable to the current process, with the notable exception that the sticker must be present on the envelope. The database record for the voter needs to be marked to indicate an absentee ballot was cast. When a voter casts an absentee ballot also casts a provisional ballot, the provisional ballot will not be counted. The ballot is separated from the envelope for canvassing.

5.2.5 Canvassing

A canvassing system for absentee and provisional ballots will be developed that reads in each optically scanned ballot to create an electronic ballot image. These electronic ballot images are aggregated with the scanned or reconciled versions of the electronic voting machine-printed paper ballots.

5.2.6 Reporting

Reports are made available by precinct for the vote totals for the combination of absentee and provisional ballots. The number of absentee and of provisional ballots is also made available by precinct.

6. 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.[45] On April 8, 2004, the San Jose Mercury News referred to our system in an editorial as a "Touch Screen Holy Grail."[46] Further demonstrations were given at the Computers, Freedom, and Privacy conference in Berkeley, California on April 23, 2004.[47] Another demonstration was given at the PlaNetwork conference in San Francisco, California on June 6, 2004.[48]

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.

7. 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.

8. 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. Arthur Keller organized the development of the software and arranged for the demonstrations. 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.

9. 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] In contrast, we propose to use a variant of Linux called Knoppix that can boot directly off a CD.

[5] 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

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

[7] 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).

[8] We propose that each polling place include a Ballot Reconciliation System (BRS) (described below) that has a sheet fed scanner for reading the bar code. The BRS has other benefits in support of auditing the system, also described below.

[9] 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

[10] *Risk Assessment Report: Diebold Accuvote-TS Voting System and Processes (redacted)*, Science Applications International Corporation SAIC-6099-2003-261, Sept. 2, 2003. See: http://www.dbm.maryland.gov/SBE

[11] Secretary of State Kevin Shelley Announces Directives To Ensure Voter Confidence in Electronic Systems, Nov. 21, 2003. See http://www.ss.ca.gov/elections/ks_dre_papers/ks_ts_press_release.pdf

[12] "E-Voting Undermined by Sloppiness," Wired News, December 17, 2003. See http://www.wired.com/news/evote/0,2645,61637,00.html?tw=wn_tophead_2

[13] Secretary of State Kevin Shelley Bans Diebold TSx for Use in November 2004 General Election, April 30, 2004. See http://www.ss.ca.gov/executive/press_releases/2004/04_030.pdf

[14] "Leahy: Unskilled workers to blame," Miami Herald, September 12, 2002.

[15] "Area Democrats say early votes miscounted," The Dallas Morning News, October 22, 2002.

[16] "Electronic Ballots Fail to Win Over Wake Voters, Election Officials, Machines Provide Improper Vote Count at Two Locations," WRAL-TV Raleigh-Durham, November 2, 2002.

[17] "ESlate voting proves smooth, not flawless," Houston Chronicle, November 5, 2003.

[18] "Polling places report light turnout here," Richmond Times-Dispatch, February 11, 2004.

[19] "Voters Decide Record Bond Issue; Edwards Quits," NBC4TV, March 2, 2004.

[20] "7,000 Orange County Voters Were Given Bad Ballots." Los Angeles Times, March 8, 2004.

[21] "Human goofs, not machines, drag vote tally into next day." Palm Beach Post, March 14, 2002.

[22] "Out of Touch: You press the screen. The machine tells you that your vote has been counted. But how can you be sure?" New Times, April 24, 2003.

[23] "Officials still searching for election glitch: The new system could not send the tabulations to the elections office." St. Petersburg Times, April 6, 2002.
[24] "Elections Chief Sees Nearly Flawless Vote." St. Petersburg Times, March 5, 2002.
[25] "Election results certified after software blamed." Albuquerque Tribune, November 19, 2002.
[26] "Montville and Chatham mayors ousted." New Jersey Star-Ledger, June 9, 2004.
[27] See http://www.wired.com/news/business/0,1367,58738,00.html
[28] See http://www.accupoll.com/News/PressReleases/2003-10-10.html
[29] See http://www.sequoiavote.com/mediadetail.php?id=74
[30] See http://www.wired.com/news/evote/0,2645,63618-2,00.html?tw=wn_story_page_next1
[31] See http://www.aitechnology.com/votetrakker2/evc308.html
[32] These systems are provided by ES&S (http://www.essvote.com/HTML/products/automark.html) and Vogue Election Products and Services (http://www.vogueelection.com/products_automark.html).
[35] See http://www.populex.com/
[36] See http://www.election.nl/
[37] Margaret Anne McGaley. *Electronic Voting: A Safety Critical System*. See http://www.redbrick.dcu.ie/~afrodite/E-Voting/Report/node18.html
[38] Election Commission of India, Electronic Voting Machine (EVM) description. See http://eci.gov.in/EVM/
[39] See http://www.smartmatic.com/electionsVenezuela2004.htm
[40] See http://www.cartercenter.org/doc874.htm
[41] See http://www.verifiedvoting.org/
[42] See http://www.accessiblesociety.org/topics/voting/electionreformlegis.html
[43] See http://www.verifiedvoting.org/
[44] 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
[45] See http://www.siliconvalley.com/mld/siliconvalley/8328014.htm
[46] See http://www.kentucky.com/mld/mercurynews/news/opinion/8383100.htm
[47] See http://cfp2004.org/program/#votingmachinedemo
[48] See http://www.planetwork.net/2004conf/program.html