# Physical Verifiability of Computer Systems

Rebecca T. Mercuri
Computer Scientist, Notable Software
P.O. Box 1166, Philadelphia, PA 19105

## Publication Note

This paper was originally published in the proceedings of the Fifth International Computer Virus and Security Conference, held March 11-13, 1992 at the New York Marriot Marquis. The DPMA Financial Industries Chapter, in cooperation with ACM-SIGSAC, CMA, COS, and the IEEE Computer Society, sponsored the event. On request, the author can provide a copy of the proceeding pages in which the paper first appeared. The version issued here consists of the entire text of the 1992 publication with some corrections that are only grammatical or cosmetic in nature. The content has not been affected in any way. The edition includes this additional Publication Note along with an Author's Comment (between the Conclusions and Bibliography sections) added in December 2005.

## Abstract

*The physical verifiability of computer-human transactions could enhance the security and auditability of many systems. The author examines the issues involved with verification of one form of trusted system, the Direct Recording Electronic (DRE) voting machine. The DRE is compared to earlier mechanical devices and other ballot counting methods, as well as to the Automated Teller Machine (ATM) in order to demonstrate the advantages of physical verifiability.*

## Introduction

There are many computer applications that require the accurate logging of a private transaction with a human. The Automated Teller Machine (ATM) comes immediately to mind, but other access-type situations (such as passkey entry into a secure facility, or permission to use a restricted database) are also possible. One other form of such system is the Direct Recording Electronic (DRE) voting machine. The DRE differs from the aforementioned applications due to the fact that in addition to the requirements for accuracy and privacy, there is the necessity to provide complete anonymity. In other words, the banking and access applications can allow tracking back to the user of the system, but the DRE must ensure that such tracking is impossible. This creates an enigma in the verification process that will be described in the later pages of this paper.

## Background to Electronic Voting

Voting is a fundamental right of the citizens in a democracy. The subject of denial or abridgment of voting rights appears in five of the twenty-six amendments to the United States Constitution. [US] As important as it is, though, our government leaves the method of administration of elections as a matter of States' rights. Every State may have

different regulations. For example, in some States a person may leave the voting booth without voting for any candidate, but in others a blank ballot might be invalid. Each State, therefore, has established a set of laws pertaining to the election process. It is important to recognize that even though voting machines are used nationwide in Federal elections (Presidential and Congressional), the States independently set the methods for approval, use, and inspection of their own equipment.

In the area of electronic voting systems (punchcard, marksense and direct recording), the Federal Election Commission (FEC), in 1990, released a set of "minimum performance, testing and security requirements that can be voluntarily adopted by State and local governments for voting systems in their jurisdictions." [FEC90] The key word to note here is *voluntary*, presently the FEC does not require, nor has every State adopted, this voluminous set of standards. Since over 50% of the votes cast, from the time of the 1988 Presidential election, have been tabulated by some form of computer system [FRE88], verifiability is becoming a matter of concern.

What is a DRE?

Tabulating systems for computerized vote counting, to date, have predominantly used punchcards and marksense ballots. These methods suffer from some of the same problems as paper (hand-counted) ballots, in that the cards can be lost or substituted, and deliberately or inadvertently damaged or voided. Furthermore, the punchcards have the problem of "hanging chad," a situation in which the small bits of paper are not fully removed from the holes when entering a vote, and they fall back into the same or different holes as the cards are handled during the counting process. [DUG88] The existence of a physical ballot that the voter can handle and examine prior to dropping it into the ballot box does provide some assurance of auditability, though. This is further enhanced if the card has printed on it the names of the candidates, and the hole or mark is associated with the ones selected. (Note that the minimal standards established by the FEC do not require that candidate's names be printed on the cards. [STD90])

In ever-increasing numbers, DRE voting systems are being introduced throughout the country. These differ from the punchcard and marksense systems in the same way that lever machines differ from paper ballots. Essentially, the vote is collected through a series of selections on the face of the machine, and the tabulation is performed internally, within the device, as the election proceeds. No receipt or confirmation (other than a visual scan of the voting surface prior to the conclusion of the vote) is given to the voter. In a section on DREs in the U.S. Department of Commerce, National Bureau of Standards document *Accuracy, Integrity and Security in Computerized Vote-Tallying*, Roy Saltman wrote [SAL88]:

> "...the voter is given some reason to believe that the desired choices have been entered correctly into the temporary storage, but no independent proof can be provided to the voter that the choices have, in fact, been entered correctly for the purpose of summarizing those choices with all others to produce vote totals."

Election districts presently using lever machines find that DREs offer a number of advantages over the mechanical units. Lever machines can weigh up to 750 lbs., and take considerably more space than do the 200 lb. DREs, so storage and transportation costs are reduced. The voters find the DREs more comparable to the lever units than the punchcards, and the expense of providing the cards is eliminated. [TRO89] Election boards complain also that the lever machines, some of which are in excess of 30 years old, are difficult to maintain and that the repairs require highly skilled workers and hard-to-obtain parts. [BAQ90] As governments seek to reduce expenditures, it is reasonable to assume that a considerable percentage of the districts presently using lever machines (close to 30% as of 1988 [FRE88]) will consider a move to DREs.

How does a DRE work?

DREs are currently manufactured by a variety of firms, some of which were previously lever machine vendors. They differ in construction and features between manufacturers, and within the same brand also vary due to State regulations. Generally the machines contain the following components:

1. A panel whereby votes may be entered (using pressure-sensitive keys or a touch screen).
2. Some indicators (typically light-emitting diodes or screen displays) showing which selections have been made.
3. One or more central processing units that control the internal operation of the machine.
4. Memory circuits that contain the object code of the software that provides the machine's functionality.
5. Other integrated circuit chips and discrete components that are part of the hardware design (this may include I/O, interrupt, timer, and other logic units).
6. A printed circuit board (or boards) on which the chips and components are installed and interconnected.
7. A power supply along with a battery back-up system in case of power loss.
8. Some mechanism for recording write-in votes (this may be an alphanumeric panel with a display unit, or a paper tape accessible through a window).
9. An operator's panel which permits verification that the machine is functioning properly, and may also allow viewing of the vote tallies at the start and end of the election session.
10. A unit that records the votes entered (may be a removable cartridge).
11. A tamper-proof case that houses the voting machine components.
12. A screen or curtain that permits the voter to use the machine in private.

Additionally, a separate electronic unit may reside at some central location for the purpose of collecting the individual machine tallies (using cartridges removed from DREs following the closing of the polls) and computing the election totals. (Note that the problem of transporting the tabulation unit, or otherwise communicating the tally, from the polls to the central vote-counting location is not addressed in this paper.)

## Differences between DREs and Lever Machines

Aside from the obvious differences of electronic and mechanical modes of operation, DREs are substantially different from lever machines. One might first think that Saltman's statement regarding the lack of proof that one's vote has been entered correctly also applies to lever machines, and in some sense it does. Certainly a gear or other component in a lever machine could slip and miss the tabulation of a vote. Indeed, the mechanism could even jam in such a way that a large sequence of votes might be omitted. But in the case of a mechanical unit, the hardware of the entire machine could be carefully examined and signs of wear significant enough to cause slippage or jamming would be observable. With DREs, it is conceivable that a computer glitch, or intermittent failure (which are known to occur at the rate of 1 in $10^{10}$ calculations) could happen in such a manner that would be undetectable yet have an effect on the vote tabulation. But the chance of this is so small as to not be too much of a concern. Furthermore, many DRE manufacturers have designed redundancy and error-checking into the circuitry used to collect the votes from the entry panel, and into the elements that contain the vote tallies, so any momentary glitch or malfunction of the machine would likely be detected.

If we assume that DREs are constructed in such a manner that machine failures are always accurately reported, then we must direct our attention to the detection of deliberate acts on a DRE by an individual or group of individuals that could "deny or abridge" the voter's rights. With a lever machine, any deliberate acts of tampering with the equipment would leave a physical trail of evidence. The correct operation of the device is observable and reproducible. It is even possible to train individuals to perform repairs, and manufacture the parts locally, so that a dependence on the vendors is unnecessary, if this is a security concern. [BAQ90] With a DRE, it is possible to affect the tabulations in a manner that may be undetectable, and irreproducible. Furthermore, certain of the components of the electronic systems may not be able to be obtained from anyone other than the original vendor, since they can contain proprietary materials (such as software). Repairs may be difficult, if not impossible, unless proprietary information (like circuit diagrams) is provided with the machines. It is conceivable that the purchaser of a DRE could be required to establish an ongoing relationship with the vendor, to maintain the proper working order of the machines. [MER91] The vendor's representatives may be necessarily permitted continued access to the machines' internals, in order to perform maintenance tasks. None of this would be of any concern, if we had some method whereby we could verify and validate the integrity of the vote tabulation by the DRE, but we are provided with nothing but assurances from the manufacturers that the machines work as intended.

## Verification and Validation

The verification of correct operation of mechanical hardware at the level of complexity of a lever machine is certainly tractable. On the other hand, the verification that an arbitrary piece of software, running on a VonNeumann architecture computational device, performs a certain task, is known to be intractable. (Indeed, various parts of the voting machine problem can be shown to be NP-complete. Those who are interested in this

subject should note the similarity of the keypress combinations to CNF-satisfiability.) [BAA88] Since correct operation is not provable, examiners are required to resort to weaker forms of verification. How this is done is, as mentioned earlier, left up to the States to decide.

Established quality assurance (QA) methods for computer system verification and validation have long been in place for most government contract work. The standards vary in accordance with the level of QA necessary in order to certify a product for use. A criticality level is assigned to components – the highest level is usually reserved for those whose failure could result in a potential loss of life. One would want to use no less care in designing our voting equipment, so the highest level of QA should be used in the examination process. In accordance with this understanding, the verification and validation procedure should include examinations of:

1. The vendor's System Requirements Document (SRD) in conjunction with the State election laws in order to ascertain conformance.
2. The System Design Document (SDD) used by the vendor to create the voting machine. This should be compared with the SRD.
3. The System Quality Assurance plan (SQA) used by the vendor to establish manufacturing process test policies, procedures and practices; reviews and audits; configuration management, security policies, procedures and practices; archiving; and supplier control.
4. The System Verification Plan (SVP) produced by the vendor, as well as those used by independent test agencies.

The FEC voluntary standards approach this level of QA, but are somewhat weak, especially in the areas that would be covered by the System Verification Plan. System verification involves both black box (exhaustive input) and white box (exhaustive path) inspections. Well-documented studies reveal that code walkthroughs can detect 30-70% of software errors, many of which cannot be found through input testing alone. [MYE79] The FEC's reluctance to recommend code examination possibly stems from the proprietary nature of the system source code. Presently, the vendors have been reluctant to reveal the details of their software – to my knowledge, none to date have provided a complete document to any independent agency for examination. In a competitive market, it is understandable that vendors would want to protect the code that operates their DREs under the cover of trade secrecy, but it may not be to the advantage of the voters to allow such protection. Certainly the vendors would be entitled to copyright and patent privileges where applicable, and these should provide enough legal grounds to secure their property. Without the source code, though, it is unlikely that a DRE could be verified and validated to current software quality assurance standards.

The source code alone is inadequate for providing a complete internal system verification. The compiler used to generate the object code must be available, and all hardware specifications must be revealed, down to the chip level. Even this may not be sufficient – Ken Thompson, in his 1984 Turing Award lecture, demonstrated how a Trojan horse could be inserted into the compiler itself. He summed this up quite simply when he said:

> "You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code." [THO84]

To quote Penelope Bonsall, director of the National Clearinghouse on Election Administration, "You've got to trust somebody, somewhere." [TRO89] The procedures used for verification and validation now appears to trust the vendor, by testing only to the functional level. The prospect of providing thorough source code and circuit examinations for DREs in each State (since the DREs do vary from State to State) is a Herculean task. This does not even begin to address the development of a methodology whereby each municipality can confirm that the code and circuitry contained in its own machines is identical to that verified by the State. One could suggest that it would be expedient for the Federal Election Commission to validate the machines, but this treads on the delicate issue of States' rights as they pertain to voting standards.

The Fallacy of Audit Trails

If we place our trust in the vendors (who do, after all, have the most to lose if their DREs are considered unreliable) we would be remiss if we did not provide some method, beyond functional testing, to insure that vote entries are being properly tallied. Numerous individuals and organizations have looked to audit trails to provide the necessary verification. [SAL88. STD90]

Our election process, by its very nature, is both secret and adversarial. The (essentially) bipartisan system provides an analogue to the checks and balances established by the branches of government. In the polling place, representatives of each party oversee the voting activities, such as inspecting the machines to see that they begin with zero vote counts, and insuring that the totals are recorded properly on the returns at the end of the voting session. (Let us ignore, for the sake of this argument, the inequities that can arise when members of the majority party appoint the minority party's inspectors.) With a DRE, indeed it is possible for the machine to print or display any arbitrary value that does not necessarily reflect that which is contained within the machine. No examination of the tabulating units is possible at all. Our checking system becomes largely procedural, rather than validatory.

Audit trails seem to provide us with a means of validating the DRE tallies. Each voter's entire ballot image can be recorded, and printed out at some later time. The vote could then be hand-tabulated and confirmed. It might even be reasonable to require that this be done in some small percentage of precincts after each election. Here the secrecy of the vote comes into question. Should the machine record the ballots in the sequence they were voted, it would be possible to determine an individual voter's ballot, by numbering each person as they enter the polls. The vendors who propose using such a system also provide for randomization of ballots within the recording unit, so as to make ballot identification unlikely.

But voting is not like using a bank ATM. In a banking transaction one is typically given a receipt. In case of discrepancy, the receipt serves as an arbiter. Difficulties can arise, but multiple physical verification checks do take place. A customer could say that an amount of cash was deposited that was larger than what was actually placed in the ATM envelope. Presumably the tellers who collect and certify the deposits have methods of dealing with these forms of discrepancies. It is also possible that a customer might request a withdrawal of some amount of cash and be given a smaller amount, with the receipt indicating that the larger sum was paid out. This places the user of the ATM in the position of questioning the reliability of what appears to be a secure system. Here, the tracking system that audits the cash that is placed into and removed from the machine would provide a second physical verification method. If bank officials were collaborating with auditors and programmers, and customers were consistently being short-changed, the number of "willing victims" would likely decrease, and the bank would lose its credibility with the public. With a voting system, the citizens have no choice as to which machines they can use, following their purchase by a municipality. One can choose a different bank, but one may not be allowed to go down the street to vote at a different polling place.

When using a DRE, one's vote is wholly private and no receipt is issued. Indeed, one might not want to provide a receipt, since then each voter would be responsible for its disposal, and its existence might encourage unscrupulous candidates to pay for votes ("turn in your receipt after the election"). Similar problems arise if the voter is issued an encrypted code number that can be used to "look up" their ballot following the election. With banking, one does want to be able to be identified with their account (unless it is in Switzerland) – whereas with voting, it is reasonable to insist that an individual should not be able to identify any specific ballot from the group, so that one's right to anonymity may not be compromised. The enigma, referred to in the introduction of this paper, is that the audit trail printout, without any form of verification that particular ballots correspond to particular ones cast, actually provides no more security than does the fox guarding the hen house.

One might then believe that the functional verification process, in issuing input sequences that are examined against the audit trail printout, guarantees that the auditing method is correct. It does not take much imagination to create a scenario in which a particular Trojan horse program is activated by a special sequence of keypresses on the DRE (the systems allow for a voter to select a candidate and then de-select it, numerous times – the ballot is not recorded until the end of vote is signaled). This Trojan horse might then increment one candidate's tally by some percentage, decrement the opponent by the same percentage, and then restructure the ballot images to make them appear legitimate. To further evade detection, the keypress sequence might be distributed over a series of voters. As the number of keys on DREs may exceed 500, it is unlikely that validation testing would inadvertently happen upon the precise trigger sequence. Again, one could require that the audit trail record the entire series of keypresses entered by each voter, but unless the order of the ballots was retained (which would violate the privacy of the vote), the sequence might be hard to reconstruct. (A common criticism of this scenario is that collusion among a group of individuals would be necessary in order to carry out this

scheme, and that this would encourage detection. One has only to read the section of retired House Speaker Tip O'Neill's autobiography which describes an early ballot rigging method involving large numbers of participants, in order to understand the ease with which far less sophisticated techniques have been widely used without repercussions. [ONE87]).

In my estimation, the only reasonable method of auditing a DRE election would involve printing each ballot before the voter exited the machine. The voter would then examine the ballot for correctness, and insert it into a ballot box. Voters would immediately be able to register a protest if the printout did not concur with the display on the DRE. Once the printout had been examined, the voter would press a key to clear the display. At the end of the voting session, the ballots would then be hand-tabulated (in a random selection of precincts), and the totals compared with the machine values. Paper ballot boxes could be impounded and used in the case of a recount. The primary difficulty that one could envision with such a system (other than the additional cost and time) would be paper jams, although recent advances in printer technology make this only a marginal concern. This method returns the verification process to the voter, and enhances the sense of trust in the DRE equipment.

## Conclusions

Physical verification provides an enhanced method for ensuring the accuracy and integrity of a private and anonymous transaction. It allows the user to become a key player in the continual certification process. The difficulty of auditing and validating elaborate computer systems, like DREs, necessitates an investigation of alternative verification methods such as those that include physical logging and confirmation.

Activities that could conceivably have requirements similar to those handled by DREs in the voting process include: confidential calls to suicide or abuse hotlines, AIDS blood test result reporting, Swiss-style banking transactions, and tracking of movements of top secret personnel without revealing their identities. Other applications are certainly possible. The discussion and solutions suggested herein for the DRE could be extended to these types of systems.

## Author's Comment (December 2005)

During the early 1990's, at the time of this publication, New York City officials were debating the replacement of their lever voting machines with a pushbutton-style of DRE. This paper was widely circulated as part of the effort to explain the numerous scientific reasons for the necessity of providing features and processes that enable independent auditing of electronic balloting equipment. Although most of the information remains valid and relevant, a small part of the content has been superseded by later research and data. Updated facts would include: over 80% of votes cast now being tabulated by computers in U.S. elections; an observed rate of 3-5% of uninstantiated vote selections and up to 9% failures of some balloting equipment in actual elections; and studies that have demonstrated marksense voting to be at least, if not more, cost-effective than DREs.

This paper was among the first (if not *the* first) to describe:

- dissimilarities between DREs and ATMs, and between DREs and lever voting machines;
- reasons why source code inspections are necessary but also insufficient in the verification and certification process;
- computational complexity issues that make functional testing inadequate in revealing equipment flaws;
- constitutional and legislative matters that preclude the possibility of uniform voting system deployment throughout the United States (or even within individual States);
- fallacies of relying on post-election printouts of stored ballot data; and
- explanations for why receipts, coding/numbering, and sequential storage or printing violates the privacy requirements of anonymous balloting.

The paper also documents some of the earliest calls for:

- application of disclosed quality assurance techniques in the certification of election equipment;
- voter choice in balloting methods (such as are now provided with no-fault absentee laws in some localities);
- (what is now known as) voter-verified paper ballots and (at least certain minimal percentages of random) manual auditing; and
- use of such printed and voter-verified ballots as the true record of the intention of the voters, for recounts and other election validation purposes.

It is hoped that the reissuance of this seminal paper will help clarify ownership issues pertaining to the intellectual property and history of the material discussed herein, and will further the understanding and development of physically verified technologies and assurance methodologies.

Bibliography


[BAA88] Baase, Sara, Computer Algorithms, 2nd Edition, Addison-Wesley, 1988.

[BAQ90] Baquet, Dean, with Gottlieb, Martin, "A Perennial Maze, New York's Election System," The New York Times, October 18-21, 1990.

[DUG88] Dugger, Ronnie, "Annals of Democracy (Voting by Computer)," The New Yorker, November 7, 1988.

[FEC90] Federal Election Commission, "FEC Approves Voluntary Computer Voting System Standards," Press Release, Washington, D.C., January 25, 1990.

[FRE88] Frenkel, Karen A., "Computers and Elections," Communications of the ACM, Volume 31, Number 10, October 1988.

[MER91] Mercuri, R. T., "Questions for Electronic Voting Machine Vendors," Urban Policy Research Institute, Election Watch, February 1991.

[MYE79] Meyers, Glenford J., The Art of Software Testing, John Wiley & Sons, 1979.

[ONE87] O'Neill, Tip, with Novak, William, Man of the House, Random House, Inc., 1987.

[SAL88] Saltman, Roy G., Accuracy, Integrity, and Security in Computerized Vote Tallying, U.S. Department of Commerce, National Bureau of Standards, NBS Special Publication 500-158, August 1988.

[STD90] Federal Election Commission, Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems, 1990.

[THO84] Thompson, Ken, "Reflections on Trusting Trust," Communications of the ACM, Volume 27, Number 8, August 1984.

[TRO89] Trombley, William, "Paper Ballots' Days May Be Numbered," Los Angeles Times, July 3, 1989.

[US] Constitution of the United States, Amendments 14, 15, 19, 24, 26.