COMPUTERIZED (DRE) ELECTIONS ARE NOT TRUSTWORTHY

by Richard D. Tucker 05 February 2007

I. INTRODUCTION.

II. GENERAL DISCUSSION -- HOW COMPUTERIZED ELECTIONS CAN FAIL.
A) BASIC ELECTION REQUIREMENTS -- ANONYMITY, ACCOUNTABILITY, AND VISIBILITY
B) TRADITIONAL ELECTION SYSTEMS
C) THE STRUCTURE OF COMPUTERIZED ELECTION SYSTEMS
COMPUTERIZED ELECTION (DRE) SYSTEMS -- ANONYMITY
COMPUTERIZED ELECTION (DRE) SYSTEMS -- ACCOUNTABILITY
COMPUTERIZED ELECTION (DRE) SYSTEMS -- VISIBILITY
D) THEY WOULD NOT DO THAT WOULD THEY?
E) COMPUTERIZED ELECTION (DRE) SYSTEMS -- FUNCTIONALLY

III. APPENDICES.
A.1. FORMAL VOTING SYSTEM REQUIREMENTS
A.2. FORMAL DESCRIPTION OF A COMPUTERIZED VOTING MACHINE

IV. REFERENCES.

==========

I. INTRODUCTION.

The information in this paper regarding computers and voting processes has been known for years, but perhaps not written in one place, at one time.

From Richard Bergholz, 1969, "Experts' Game: How Elections Can Be Rigged Via Computers" to Roy G. Saltman, 2006, "Independent Verification: Essential Action to Assure Integrity in the Voting Process", the short-comings of computerized elections have been announced, and then seemingly glossed over (by a long discussion, if necessary). (See References.) For each level of electronic voting machine, computer professionals have admitted that the "current" version of such machines fail; and then typically add "...but if you hire me as a consultant, we can fix that."

Such is not the case. Computerized elections are not trustworthy -- and can not be made trustworthy. Trustworthiness is crucial, because the winner of some offices (Governor or President) then takes effective control of the "legal apparatus" -- the police and the attorney general -- which would investigate and prosecute any fraud. This is in contrast to typical fraud cases, where the victim expects to be heard in a "neutral" court of law.

Governmental elections require Anonymity, Accountability, and Visibility. Traditional voting systems have their own strengths and short-comings, but using a highly computerized voting process (DRE) will partially solve some voting issues. However, it adds a wide range of computer-related problems, compromising the required Anonymity, Accountability, and Visibility. Computers are very adaptable, and that characteristic is a "feature" in some environments, but it is a "fault" in voting systems.

==========

II. GENERAL DISCUSSION -- HOW COMPUTERIZED ELECTIONS CAN FAIL.

A) BASIC ELECTION REQUIREMENTS -- ANONYMITY, ACCOUNTABILITY, AND VISIBILITY

In the past, there have been failures in public elections. This includes bought votes, "hanging chads", tampering with mechanical voting machines, stuffed ballot boxes, and discarded ballots. Public trust in an election hinges on the open viewing of the election process and the confidence that any substantial failure in the voting process will be become public.

There are three basic balloting requirements for any significant election --
1) a secret ballot (Anonymity),
2) an accurate counting of those ballots (Accountability), and
3) transparency of the process (Visibility).

Observe, first, that "Anonymity" and "Accountability" are MUTUALLY EXCLUSIVE. Any action which ensures or promotes one of them will prevent or interfere with the other. If a process ensures Anonymity of the ballot (i.e., "the secret ballot"), then the counting process (Accountability) is less trustworthy (easier to cheat upon, without getting caught). If a process increases Accountability (tracking information), then it destroys Anonymity (the secret ballot).

Because of this conflict, the voting process must not only be Visible to the voting public, but also the interaction, or interface, between Accountability and Anonymity must be clear, as well. Any lack of this Visibility in the election process will call into question both the Accountability and the Anonymity of votes. Public confidence in an election, both the process and the results, is tied to directly observing, during the election, precisely how Accountability and Anonymity requirements are implemented, and how they interact.

There must be confidence that if there is a failure -- either by accident or by intent -- then the failure will at least be detected. Election officals may be subject to criticism and possible legal action if open, observable, and well-defined election processes are not carried out.

B) TRADITIONAL ELECTION SYSTEMS

In a "traditional" election, rules and processes have evolved to reduce cheating and allow the electorate to trust the outcome. The traditional voting process attempts to clearly deal with "Anonymity" and "Accountability" as mutually exclusive processes.

Typically --
1) A voter registers beforehand, allowing a registrar to check the information and prevent someone from registering in two precincts at the same time. On election day, voting lists are sent to each precinct. (Accountability)

2) A voter signs in at the polling place and takes a ballot. (Accountability)

3) A voter goes to a generally viewable area (Accountability), and marks the ballot, but out of sight of direct viewing. (Anonymity)

4) A voter folds the ballot or places it in an envelope (Anonymity) and deposits it in a ballot box in general view. (Accountability) The ballots mix, unseen, within the ballot box. (Anonymity) The ballot box is closed. (Accountability)

5) At the end of the day, and with multiple witnesses, the ballot box is opened at each precinct, and the ballots are counted. (Accountability)

6) The precinct counts are aggregated into final counts. (Accountability)

7) If there are any questions afterward, then the ballots are phyically available for individual inspection and recount. (Accountability)

The above process is "Visible" (transparent), and the few transitions between "Anonymity" and "Accountability" are clear and viewable. If this clarity of process is not followed, election officals are open to criticism and legal action.

This voting process can be viewed as a series of colored boulders or stepping stones -- one color for "Anonymity" and a different color for "Accountability". As a voter steps through the process, he knows clearly where he is in the process -- that is, what color of boulder he is stepping to or from.

C) THE STRUCTURE OF COMPUTERIZED ELECTION SYSTEMS

Computer controlled elections are typically called "Direct Recording of Elections" or "DRE". Discussions of Computerized Elections usually focus on only one part of the process -- the "User Interface", the secret ballot (Anonymity), or how the votes are collected (Accountability). These discussions avoid dealing with the combination of Anonymity, Accountability, and Visibility.

COMPUTERIZED ELECTION (DRE) SYSTEMS -- ANONYMITY

The secret ballot, Anonymity of the voter, is a permanent problem for Computerized Elections (DRE) machinery. Computers are phenomonal record "keeping" devices. A voter would not know if a finger-print, picture, or identification tag is being observed and stored, along with his vote. Such a tag can be stored in a database, and then be used later to connect a voter with a ballot.

For example, the "Vote Now" button can include finger-print reading hardware. (To receive a California State Driver's License requires giving a digitized thumb-print to the State.) Computerized finger-print security hardware is readily available. Also, tiny cameras can be imbedded in the equipment -- ones like the camera found in many "cell phones".

Sequence numbers, RFID tags (Radio Frequency IDentification tags), or timestamps can also form a surreptitious link to break down parts of the voting process which were meant to ensure Anonymity. These identifiers can be held in a succession of tables, no single table sufficient to track a voter. But if collected together afterward, the tables would provide end-to-end tracking of a voter and his vote.

Alternatively, if Anonymity of voting is truly guaranteed, then enough "Anonymous", non-trackable, votes may be generated by the computer to alter an outcome, but not enough extra votes to raise suspicions.

COMPUTERIZED ELECTION (DRE) SYSTEMS -- ACCOUNTABILITY

Computerized Elections (DRE) leave a voter unsure of whether the ballot is being recorded, transmitted, and tabulated correctly.

If a failure in the process happens, the failure will not likely be detected, and if it is detected, it will not likely be corrected. If the failure is planned from within the the manufacturer, the chance of discovery is miniscule. If such a malevolent failure is discovered, it can be declared a "programming error". The effect, and any attempt to discuss the failure, can be summarily dismissed.

Generating paper copies of ballots AFTER the polls close does not help Accountablity. (Some electronic voting machines do produce paper afterward.) The changing of votes could be accomplished between the time the person voted and the time the printing is carried out. The printout would reflect the falsified version.

A "Voter Verifiable" voting machine produces a written record, which is checked and verified by the voter, and which is the only "official" ballot. The ballot then drops into a box, when the voter is "satisfied". But this process only partially solves the problem. If a voter fills out the ballot quickly, then the computer could print the ballot as requested. But if the voter works slowly, indicating confusion, then the computer could change crucial votes, unlikely to be caught during the "Verification" step. In any case, on a long ballot, many people would fail to catch a change improperly made by the computer. Verifying the ballot is difficult even if the voter has a sample ballot, filled out beforehand -- and even if it "looks" like the ballot which will be "Verified".

COMPUTERIZED ELECTION (DRE) SYSTEMS -- VISIBILITY

In a commercial (rather than a voting) environment, if computerized fraud takes place, the person or group defrauded has at least some chance of taking the matter to court. But so much is hidden by computerized voting that either detecting fraud or recovering from voting fraud is very difficult. At the national level (and in some states) the winner of a top office (President or Governor) soon takes effective control of the "legal apparatus" -- the police and the attorney general. The winner can then assign his own appointees to (not) investigate and (not) prosecute.

Computerized Elections are NOT "transparent". Superficially, the computer may tell the voter what is happening. But as the voter steps through the voting process, it is NOT clear which activities ensure "Anonymity", nor which activities ensure "Accountability".

The voting process can be viewed as a series of colored boulders or stepping stones. Then, in this computerized environment, "Anonymity" and "Accountability" are no more than colored grains of sand, blowing about the voter's feet. In reality, even the colored sand can not be seen.

Visibility of the process is important. In the U.S. 2000 Presidental Election, the U.S. Supreme Court did the actual choosing of the next President. However, because details about the actual votes and the voter registration processes were available, people around the world could draw their own conclusions about the American "democratic process".

D) THEY WOULD NOT DO THAT, WOULD THEY?

There is some indication that a variant of the above scheme to miscast electronic votes has already been used:

The electronic voting machine provides balloting information for well known (important) offices and issues. These would be ones which the voter would immediately notice and would complain if the item did not appear. On the basis of a voter's previous selections, the machine may or may not provide a less well known office or issue. That is, if the voter is expected to vote in the "approved" manner, then the item would be displayed to the voter, and the voter would make a choice. However, if the voter was expected to vote in a "not approved" manner, then the item would not be presented, and the voting machine could select the "approved" choice, but not tell the voter.

If this cheating were done on a random basis, some voters on both sides of the issue would remember voting without a problem. Even if the voter asks to review the ballot at the end, hidden choices might not be presented. If the voter specifically asks to return to the selection area, the voting machine could then allow the previously hidden item to be viewed and voted upon. Some voters would catch the cheating, but they would have to admit they ultimately got their choice. Some voters would NOT catch the cheating, but they would later have only a hazy recollection of not voting on a specific item.

On a long or complex ballot, this method of cheating would be particularly successful. People would forget which way they voted on a specific item. In this case, even a voter-verifiable "printed receipt" version of the ballot (then kept by the voting machine) would be long and complex enough to successfully cheat a significant number of voters. If the voter had a "sample" ballot, previously filled out by the voter, which appeared identical to the one printed by the computer, then the voter would have a chance of catching errors. However, at least some California electronic ballots have been substantially different than "sample" ballots. But this would be only a partial cure -- the issue of a proper "secret" ballot is still an open problem.

E) COMPUTERIZED ELECTION (DRE) SYSTEMS -- FUNCTIONALLY

This is a general description of how a computer works, which should be understandable by a computer-literate person, but not necessarily the general public.

General computer systems, including the ones used in Computerized Elections, are made up of many layers of software, as well as multiple layers of "hardware". Each layer of software has opportunities for errors (mistakes by the original programmers) as well as opportunities for intentional malfeasance.

Computer programs are prone to "upgrades" and "corrections", which are ideal times to insert malicious code. If the malicious programming is discovered, it is declared to be an error; and it may be fixed or simply moved to another spot in the program. The boundaries between layers of software are often weak points in a program or system, prone to error and vulnerable to both attack and malicious manipulation.

A typical, current, DRE system can, in fact, talk to (or be attacked by) any other computer on the Internet. (A couple of manufacturers bidding for a Santa Clara County contract were very proud of this "feature".) It can give out information about how people are voting. It can receive commands to change its internal programming code, which might change votes that have happened in the past or votes that will happen in the future.

A given layer of software may contain millions of lines of computer code. At the top, the application -- driving what the voter sees -- calls its own procedures and libraries (usually, dozens of them). Any of this can call system libraries and routines (which call any number of other routines), as well as system calls that talk to programs and computers in other places. The system itself gets control (whether the application likes it or not) to do what it wants (call more routines and libraries), whether those calls relate to the application's tasks or not. Most of the Computerized Election computer systems go automatically to the Internet, presumably to talk to some main host.

Even the computer "hardware" is not "hard". It is certainly possible for even the basic "hardware" to work one way during testing, and work another way on election day. In the early days of computers, "hardware" was "hard" -- it consisted of circuit boards, wires and electrical devices. Modern computers are NOT "hard" electrical devices, but typically contain "micro-code" devices (sometimes derisively called "mush-ware"). The "Central Processing Unit" (CPU) -- a "microprocessor" -- is, itself, layers of computer programs (microcode), as well as the underlying "hard" stuff. Many microprocessors are capable of changing, or reloading, the (micro)programs that drive their inner workings.

==========

III. APPENDICES.

A.1. FORMAL VOTING SYSTEM REQUIREMENTS

A Trustworthy Election has these requirements:

A. Secret ballot (Anonymity) --
Given the collection of voters and the collection of ballots --
1. a voter can not be identified with a given ballot or choice;
2. a ballot or choice can not be identified with a given voter.

B. Accurate tabulation (Accountability) --
1. People authorized to vote are allowed to vote.
   a) No denial or deletion of valid registration.
   b) No denial of voting process.

2. No multiple registration or phantom voters.

3. Each voter votes once.

4. Each vote is accurately tablulated --
   a) A vote cast for an Item is counted for that Item, in the manner the voter intended.
   b) No votes are deleted (not counted) for some Items.
      (An audit will not catch this problem, because the voter might have actually chosen to NOT vote for this office or proposition.)
   c) Votes are not shifted from one Item to another -- this activity will escape detection in some types of audit.
      1) Shift votes from Item A to Item B, to help B and hurt A.
         (This may draw attention, if A is thought to be more popular than B.)
      2) Shift votes from Item A to Item C to help B and hurt A.
         (If there are multiple Items (candidates) for a given election (office), and plurality (50%) is NOT required, then B has a better chance of winning, and votes for C are seen as a "protest

vote", thereby not arousing suspicions of a "rigged" election. If plurality (50%) IS required, then if A, B, and C are reasonably close, this shifting may cause an otherwise "favorite" A to place third, allowing B to have a runoff election with C, rather than with A.)

C. Transparency of the process (Visibility).
1. Voting process must be Visible to the voting public.
2. The interaction between Accountability and Anonymity must be clear.
3. Confidence that any failure of the process will, at least, be detected.

A.2. FORMAL DESCRIPTION OF A COMPUTERIZED VOTING MACHINE

This description relates to "dependable output" for a voting machine. As such, it addresses both the issue of a secret ballot (Anonymity -- NOT keeping track of who is voting) and the issue of accurate tabulation (Accountability -- correctly counting the votes). It also describes lack of transparency of the process (Visibility).

Realistically, a computerized (electronic) voting machine (DRE) is a composite of an application, an operating system, and at least two layers of "hardware" (microcode plus physical hardware).

Each layer represents a mapping on a set of command data (domain), producing data effects (range).

The process of a computerized voting machine is, therefore, a composite mapping:

H(Os(A[P,La,V], Lo), M]), where
H is the physical Hardware (silicon chips, et al).
This is directed by the software instructions and by
M, the Microcode (which controls what to do with each "software" instruction).
Os is the Operating System function, which processes the Application, A, using
Lo, the Operating System Libraries.
A is the computer "Application", which processes
P, the computer Program,
La, the Application Libraries, and
V, the Voter input.

For this process to be accurate, each part of the composite must be a proper mapping.

The raw Hardware is invariably proprietary, and therefore not publicly checked or verified. It can have its own design and construction errors. The hardware dependability can even be affected by its speed and its operating voltage. Of the four "mappings", this operation typically comes the closest to being a valid "mapping".

The Microcode is merely a set of proprietary software, which uses one set of hardware to emulate another set of hardware. This software can often be modified "on the fly", so that the "hardware" works one way at one time, and it works differently at another time. (There are times this is desireable -- but not in a voting machine.) The altered behavior would be nearly impossible to detect. Like other "software", microcode can have its own "bugs" and errors. Since multiple versions of the microcode may

be stored within its own internal memory, the microcode operation is potentially multivalued, and can not be considered a proper mapping.

The Operating system is a complex set of software. Verifying that the operating system is truly what it claims to be is nearly impossible. If it did exactly what it claims to do, it would have no errors, or "bugs", which is not likely. Even an "open", inspectable operating system would be large enough to have bugs, and it would be difficult to check for "intent". An operating system is usually too complex to be considered a proper mapping.

The Application software provides the voter-user interface and the administration-user interface. (The voting administrator who oversees the voting process is as much of a "user" as the voter.) The Application software provides the computer's instructions for gathering and communicating the votes. If the software is proprietary, it is not subject to public scrutiny, and, therefore, portions may work one way during testing, and differently on election day. Even non-proprietary code can easily be obscure enough to be untrustworthy. In either case (proprietary or non-proprietary), most sophisticated applications are complex enough to have accidental errors. There are corporations which claim to "prove" software applications. However, such "proofs" assume that the operating system and "hardware" work "as advertised". But without a guaranteed "Hardware"/"Operating System" underlayment, it would be difficult to claim the results of the Application software is a proper mapping.

Because the pieces of the composite function are potentially multi-valued, and not proper mappings, the composite funtion is not a single-valued (trustworthy) mapping from the votes intended (cast) to the votes expressed (counted).

==========

IV. REFERENCES.

Saltman, Roy G., August 22, 2006, Independent Verification: Essential Action to Assure Integrity in the Voting Process, National Institute of Standards and Technology (NIST), under Order No. SB134106W0703.
This references the following, Richard Bergholz, 1969, among others.

Bergholz, Richard, 1969, "Experts' Game: How Elections Can Be Rigged Via Computers," Los Angeles Times, July 8, p. 1.

==========

Note: This (05 February 2007) is the 2nd edition of this paper.
The first edition was 27 October 2006.

Copyright (C) 2007, Richard D. Tucker
Verbatim copying and distribution of this entire article is permitted in any medium, provided this notice is preserved.
