

Doug Lewis testimony before the California Secretary of State's Ad Hoc Committee on Voter Verified Paper Ballots

The Election Center

An international association of voter registration and election officials
12543 Westella, Suite 100
Houston, TX 77077
Phone: 281-293-0101
Fax: 281-293-0453

Email: electioncent@pdq.net

Website: www.electioncenter.org

Now that Direct Recording Equipment (DRE) voting systems are growing in acceptance and use in American elections, it is almost inevitable that some groups, individuals and organizations will claim that such systems are not safe enough to use in elections.

And this argument is not new. When lever machines were first introduced into the elections process, all those favored paper used the same kinds of arguments. When IBM first started computer counted punchcard voting, many of the same kinds of arguments were made.

Because DRE's represent another shift in the kinds of technology used for elections, we see the renewed fears of introducing the newer technology. It is entirely normal for these arguments to arise as we shift to a generational change in the types of voting systems used.

The problem is that well intentioned people, some of them even highly educated and respected, scare voters and public officials with claims that the voting equipment and/or its software can be manipulated to change the outcome of elections. And, the claim is, it can do so without anyone discovering the theft of votes.

Since so many people tend to distrust technology they have limited knowledge about, it only makes the situation worse.

Let's confront the problem directly: it is highly probable that any machine devised by humans can be broken by humans. So ANY technological argument to the contrary seems to be doomed from the very beginning. We can take precautions, we can make it more difficult, but the end analysis is that you cannot build a totally secure voting device.

The real question is, can you gain access to the software, change it, have it manipulate the results for one or more races, have it not be evident when you do the pre-election test, erase itself before the post election test, and get away with it totally undetected?

As usual, this all boils down to appropriate election policies and procedures, and with an understanding of what it would take to do all of the above and get away with it without anyone discovering what you did (or attempted).

Voters need to know that even if the election official is sloppy about some procedures, that it is still improbable (vs. impossible) a "rogue

vendor" could act alone to change election results (to use an allegation that has been made).

Here are the steps that a person would have to go through to be able to change the outcome of an election.

- A) You have to know the language the software was written in (not English, Spanish, etc., but rather the programming language)
- B) You have to know every location in the software where it checks on itself to verify that the numbers it is reporting are accurate;
- C) You have to know the language AND VERSION of the compiler that was used to compile the program (it converts the program from a human readable form to machine language)... in order to "reverse engineer" the software you must have the identical version of the compiler in order to reverse engineer it;
- D) You have to gain access to the software for a long enough period to actually replace it;
- E) You have to make the software ignore the pre-election test or tests and only initiate itself on election day;
- F) You have to have the software be able to actually change votes throughout the day and do so undetected;
- G) The software must be able to erase or conceal itself before any post-election test.
- H) If the software is programmed onto a ROM (Read Only Memory) chip then you have to have physical access to the units.
- I) With access to the units, you must be able to remove enough of the ROMs in the units to reprogram them. This entails having enough time to either erase the ROMs installed in the units or having enough supplies of identical ROMs that you can have them preprogrammed and inserted into the units... all undetected.
- J) You then have to have access a second time to remove the "malignant" ROMs after the election and replace them with the real ones you removed (so that you can get away with the election fraud undetected).
- K) You have to do this not only on enough machines in one jurisdiction (unless your intent is to manipulate a local election - and why would anyone take these kinds of risks for a County Commissioner's race, or Sheriff's race or Mayor's race?), but in many jurisdictions in order to steal a Congressional race or state race? And for the presidency, this would involve thousands and thousands of people...unless of course we go to one system nationally (or Internet voting).
- L) In states with multiple vendors of DRE's it means that you have to go through the entire process for EACH type of DRE (and still be able to get away with it).
- M) Even in Central processing of election results through an Election Management Software package, you still have the individual results of local precincts (and each unit therein) and can verify the results as reported by them in comparison with the Election Management System results.
- N) In many states, there is a requirement to escrow the software, so that you can compare the software in the units with the escrowed software.
- O) Even in states where this is not so, NASED requires the ITAs to escrow the software at the ITA (Independent Test Authority) so it can be compared to the originally qualified software.
- P) You now have to have the involvement not just of one or two

people but significant numbers of folks to make all this happen undetected, actually change the outcome, and get someone elected who should not have been elected.

Q) A piece of paper that the voter sees does not guarantee that the same results will be recorded within the machine - if you want to manipulate the election, show the voter whatever the voter wants to see and still manipulate it later. Security experts will still argue the value of having paper for recounts.

R) The current solutions presented by the vendors as a result of their concerns for the validity of the results have their own limitations, because:

a. They add a printer, which can run on ink, ribbon, or paper

b. Paper can jam

c. Printer can be disconnected from power source

(All of these mean having to repair the units during an election with repetitive jams, running out of paper, or ink, etc).

d. They add weight to the units (complicating precinct setup, shifting control of delivery and setup from poll workers to expensive delivery services along with quality control and security efforts over those services).

e. Voters can, and probably will, walk off with ballots with some of the solutions presented (vote buying?)

f. Inability of blind voters to check their ballots (Braille printing only covers 10 percent of the blind).

g. They add significant cost and complexity to the voting unit and to the skills required to support them in a voting location.

h. While the voting system may accurately reflect how the voter has voted and print an accurate reflection of that vote as a receipt, what happens when the voter has electronically "cast" the ballot but now claims the printed receipt is different? You now introduce serious credibility claims that can irreparably damage the elections process...and they will insist on keeping the printed ballot as evidence of "fraudulent programming of the machines."

i. Or, once printed receipts leave the polling site (which will be difficult to prevent at the precinct level) do you now introduce the ability of fraudulent reproduction of printed receipts intended to confuse and contrive the process?

The point is simply this: do not be misled into believing that elections are reliant upon technology which can be manipulated. The real question of whether there "are sufficient and proper safeguards to make it highly improbable?" And the answer to that is yes. It may be possible to do many things, but like time travel (which is theoretically possible), it is highly unlikely at this time.

Each of the systems is programmed at the LOCAL level. It is true that each local election is using the same base machine operating system but it is individually programmed locally. Manipulation of races for national or statewide offices or regional offices (Congress, state legislature) is far more difficult because it is highly unlikely that each of those races will appear in the IDENTICAL byte spot on each machine and would vary from one local jurisdiction to the next.

Another allegation made by some is that the software should be in the public domain rather than proprietary, leaving the impression that the software is secretly controlled by a company or individual. Simply

because the software is not open to every hacker in the world, does not mean the software is not reviewed and exposed to public scrutiny.

The national testing program for the National Association of State Election Directors (NASED) requires that the manufacturer's software must be escrowed with its written source code. The difference here is that the source code is NOT secret. It is simply unavailable to the general public -- and that is a significant difference. There are many technologically advanced people who would love to have the opportunity to examine all kinds of software (not just that used in voting) but it is not within their purview to be able to do so. Should we open all of the software available simply because they are interested?

Since the source code is escrowed with our national Independent Testing Authorities, and additionally as a condition of approval in many states or local jurisdictions, it is not secret code. In an appropriate governmental investigation or court inquiry, it can be compared from the machine to the escrowed versions. This is an appropriate safeguard for the public interest.

Additionally, the nation's ITAs REQUIRE that they witness the build of the software so they can assure an added layer of precaution is built into software security.

The genius of the American democratic process is its diversity. Since we use so many different types of voting equipment, provided by so many different vendors, and because elections are controlled by so many local elections offices, it makes manipulating an election in America very difficult.

The ability to manipulate an election with DREs, combined with election practices and procedures, means it is highly unlikely to be able to do this and get away with it. You can still manipulate an election easiest with hand-counted paper ballots. The reality of a discussion on the technological possibilities of manipulation is that no one is ever satisfied with the technological arguments or counterpoints. For every technological challenge there is a technological solution or counter challenge, none of which ever satisfy the other parties. It has to be proven that such challenges can be carried out successfully without possibility of detection when you combine the technological aspects with established testing procedures, election management procedures and public scrutiny of elections.

We appreciate and respect those who question the process and we understand their fears. And we do not take their concerns lightly. While conducting elections is likely to be an imperfect process, it is a process built upon more than 200 years of experience in how to provide appropriate safeguards. Like most situations in the electoral process, it rarely boils down to a technological issue. It almost always comes down to policies, procedures and people doing what they are supposed to do.