Can Computerized Election Systems Help?

by Stanley Ezrol, January 23, 2004

Computerized elections systems have been widely promoted in the wake of the year 2000 Florida Presidential vote count fiasco. This study analyzes the actual utility of the kinds of systems proposed as a remedy to the problem of insecure, inaccurately counted, and difficult to administer elections. It concludes that the most widely promoted new systems make a mockery of the idea of secure, verifiable election results, but that even the best of them are useless in guaranteeing fair elections without a total revolution in the quality of citizen access to the process of election administration.

There are three major types of computer elections system now in use (aside from the notorious punch card reader systems, which have lost all credibility).

Optical scanned ballots.

In these systems the voter fills out a ballot, often with a special pen, and then feeds it into a "ballot box." This ballot box may include an optical scanner and computer which adds the ballot entries to its tabulation as it is fed in, or it may be simply a ballot box.

In the former case, the tabulation computed from each machine is transmitted, either electronically (via dial-up modem, internet, or other means), or by carrying an SD card or other memory element on which the totals are stored, to a central location. At the central location, a computer tabulates results from all machines to produce the overall election totals.

In the latter case, the ballots are transported to the central location, where they are all run through a scanner and tabulated.

Direct Record Entry

The best known systems of this type are the popular touch screen systems, but it also includes audio/voice systems, push button systems, and any system where the voter directly enters his choice into a computer, without using a paper ballot.

As with the optical scanners, totals are either telecommunicated, or physically transported on memory elements for central tabulation.

These pure DRE systems are pure believe it or not. The total for the election can be checked against the total for each machine, but there is nothing whatsoever against which the total produced by each machine can be verified.

Direct Record Entry with Audit Log

These are systems in which the Direct Entry procedure includes printing either a ballot, or other paper record, for each voter. There are proposals that this procedure be used so that the printed result can be displayed to the voter, who may then accept or reject it, prior to finalizing his vote.

Which is the Most Secure?

Optical Scan ballots provide a possibility for a physical recount of the vote, with the proviso, as in all paper ballot systems, that the ballots are properly secured and stored. Similarly, if the Audit Log or ballot printed by the DRE/Printer systems, is verified by each voter, that also provides an audit record. Putting aside the question of how many voters will actually verify their votes, the problem with the latter is that, no matter how reliable the thermal printing systems in use may be, printers do jam, run out of paper, ink, etc. With thousands of machines in use intensively, after a hasty election eve set up, malfunctions are inevitable.

Computer Systems, in General

Before dealing with specifics of voting systems, and potential problems with them, some fundamental knowledge of what computers do, and cannot do, is essential:

Computers store numbers, letters, other symbols, music, photos, videos, and so on, as a series of "off" or "on" electronic or magnetic charges. This is what is called "digital" data. Since digital data consists of a specific sequence of these offs and ons, with nothing fancy, no tricks allowed, no gradations of shading or value, it can be {precisely} copied or recreated so that it is entirely indistinguishable from the original (which is the great virtue of digital sounds, images, and combinations of the two.)

A computer can recognize digital data and can produce more digital data by applying digital rules, generally contained in what is called software, to the digital "information" presented to it.

What this means is that all computerized information and software is eminently copyable, recreatable, counterfeitable, and alterable, such that there is no automatic way to detect the fraud. A computer cannot distinguish "good" software from "bad" software. If a piece of software, called for instance, "Vote Totaling Software," is copied to a computer, and if it follows the right format rules, etc., then when the computer is commanded to total votes, it will follow the rules in that software, without any possible regard for the correctness, honesty, morality, or wisdom of those rules.

Most computer "controls" on things like the validity of software or data, involve things like "checksums," or special embedded codes created according to specified rules. The computer can check the "checksum" or identifying code, and reject data as invalid. But, anyone who knows the rules for creating these codes can avoid this type of detection. Similarly, software and other data may be stored in several pieces which have to match in some way. Changing one piece without correctly changing the others may make it non-operational, but, again, if you know the rules, this is not an obstacle.

Also, computerized information may be "encrypted," particularly for transmission over phone lines, or over the internet, where it may be available to unwanted third parties. "Encryption" merely means applying some rule for scrambling the data at one end, and reversing the procedure at the other end to return it to its original state. This procedure may include the use of one or more "keys," which are known by the scrambler and unscrambler, but not transmitted with the data. The contents of these keys are incorporated in the scramble/unscramble procedures. Thus, encryption can be used not only to scramble the data, rendering it unintelligible in that state, but can be used to certify that it is from a valid source (one with the right key). If, as is often the case, the encryption routines are widely available commercial routines, anyone who gains access to the keys can decode the encrypted messages.

Computer software consists of "operating system" software and "application" software. There is no strictly defined division between the two. Operating systems are software for controlling routine computer operations such as reading and writing data to magnetic disks or other mediums, displaying data on video screens, recognizing data typed on keyboards, etc. Internet browsers, dialers for telephone connection, word processors, spread-sheets, photo editing, movie editing, and other special purpose software is also, typically included with "Operating" software such as Microsoft Windows. Application software is software provided for some special task: accounting, voting, vote tabulating, etc., which are special requirements not common to all computers.

As far as we know, all of the major elections systems use some version of Microsoft Windows for both the voting and central tabulation machine operating systems.

Windows and Windows application software is highly complex, and highly difficult to keep track of. Each version of "Windows," for instance, consists of tens of thousands of separate computer "files" (a file simply being a specific named collection of digital data), scattered over several "folders" on the computer hard drive. Application software can consist of anywhere from several to hundreds or thousands of separate files.

When you run or execute a "program" on a Windows computer, the computer starts following the instructions in one of these files. Those instructions will include reading data from other files, from the Windows Registry (A file generally not accessed by, nor understood by, computer users. Amongst other things, it contains data used by programs, which can alter what the programs do. That is, the precise same software may function differently depending on what it finds in the Registry.), and from ".ini" files (text files which, like the registry, programs use to store data on what they should do on that particular computer, or for that particular user). It will also invoke other programs to perform certain functions. Amongst these other programs, are those stored in ".dll" files. If you're not familiar with these, and have access to a Windows computer, search for files with .dll in their name, and you may be shocked at how many there are.

The proper functioning of Windows software, then, depends on having the correct versions of tens of thousands of program and .dll files, the correct Registry settings, the correct .ini and other data values, and so forth. Neither Microsoft, nor most software vendors, systematically instruct a user on which .dll or .ini files, nor which registry entries are required. Typically, the only way a computer user (including the experts), knows what a particular .dll does, is when something doesn't work. Trouble-shooting guides may direct them to the out of date, missing, or corrupted .dll, registry entry, or what not. As long as everything seems to be functioning all right, these things are invisible.

There is absolutely no way to constantly guarantee that the software on a Windows computer is exactly what it is supposed to be.

Windows “Security”

Windows was initially designed as an operating system for a single user hobbyist's computer, doing one thing at a time. Windows Systems up through Windows 98 had NO security whatsoever. A user sits down, turns it on, and has full access to everything on the computer. Individual software applications might have required passwords for use, but that doesn't prevent someone from using the software, it just forces him to figure out how to set up a password for himself.

In practice, the security features of later Windows versions are so cumbersome, and so difficult to “tune” to permit necessary operations, while restricting others, that they are often not used. Recent celebrated cases, like CIA Director John Deutsch copying files from work to his home computer, or the Los Alamos scientists who routinely copied their work to floppy disks because they didn't trust the network “backup” operations, make it clear that computer security is simply not taken very seriously, even where it would seem to be most critical. Even if Windows security is used, it is dysfunctional. Virtually every week, Microsoft provides software “Updates” required to defend against “security vulnerabilities,” often including the possibility that a third party can take total control of your computer system.

Aside from outside “hackers,” any computer system must have administrators who have complete access to read, destroy, or alter any data on the computer. Since software development and testing often requires the ability to make sure that software, hardware, and so on, is functioning correctly, in all but the largest software operations, most software developers, trouble-shooters, and so on, will have full “administrator” access to computer systems. This is why, today, computer operators turn up as spies along with the communications personnel.

The Internet

Over the last decade, Windows has become intimately intertwined with the Internet. It is very difficult to operate a computer system in isolation from the Internet. Windows is constantly being upgraded, revised, fixed, and so forth. Direct connection to the Internet is the only convenient way provided by Microsoft to keep their software updated. This is also generally true for application software vendors. Connection to the internet is almost always the preferred route, and, in some cases, the only way for installing or upgrading software, or registering it with the vendor to make it legally usable. Many software products only make instructions and “help” available through the internet. Some products, including Microsoft's SQL Server database software, which don't intrinsically have anything to do with the Internet, nonetheless require that Internet browsing software be installed, and that the Internet communications protocols (TCP/IP) be in use.

Commercial and government users who may shield their most sensitive systems from the internet, generally will, nonetheless, use software or data downloaded from the internet, which they transfer by floppy disk, CD or other means, to their “secure” computer. Some of these users don't even realize that having a computer on a network with other computers which access the internet, also exposes them to the internet.

Although none of these elections systems are supposed to be connected to the internet during the conduct of an election, internet connections are used in the setup and counting--sometimes to transmit totals for central tabulations, and possibly to receive software updates.

The Internet protocols (rules whereby computers communicate with each other), and the initial communications infrastructure of the Internet were developed by the Pentagon's Defense Advanced Research Projects Agency (DARPA). The up-front mission of the Internet was to make it possible for people scattered in various academic and government institutions, to work on each other's computers. Snoopability was, apparently, a lesser publicized part of that mission. Hence, connecting to the Internet, by design, does precisely what no sane computer user would want to do: It announces to every other computer on the Internet, "Here I am, use me as you please."

Since the Internet has expanded beyond DARPA, attempts have been made to limit unwanted control by "alien" computers, but, as I indicated above, these controls are flawed. Prior to the Internet, systems for electronic communication between computers generally involved transmission only of individually specified data items. Other information stored on the computer was simply not available for communication. The reverse is true with the Internet: Only specified items are excluded from view to the rest of the internet.

Computerized Elections Systems

Computerized Elections Systems are promoted, largely, for two reasons. First, paper ballots are expensive and otherwise difficult to print, count, and store. Also, as highlighted by the notorious "Hanging chads of Florida," mechanical counting, and hand-counting of ballots can be unreliable. A secondary argument is that audio DRE systems can make it possible for blind voters to vote unassisted. (Although the Help America Vote Act of 2002--HAVA-- talks generally of making voting accessible to the handicapped, I have seen no mention of any handicap other than blindness addressed by these systems.) Some of the claims seem to indicate that "touch screen" systems can help the blind, but they don't explain how. Beefing up the integrity of DRE systems by displaying a printed ballot to the voter for verification, of course, won't make it possible for the blind to verify their vote.

The proposed alternatives are: optically counted paper ballots (the optical scan system); or totally paperless systems in which the voter's choice is directly recorded by a computer system (DRE); or DRE systems which produce a printed ballot or audit report.

Elections systems manufacturers, and the elections officials who are buying their products, argue that computerized systems, properly administered, can reliably record and tabulate votes. There is, however, extensive documentation on specific vulnerabilities of these systems to accidental or deliberate tampering with the vote totals.

As you can read in the documentation section [*not included with this sample*], many specific remedies for specific vulnerabilities are proposed, but it should already be clear, based on understanding the fundamental limitations of digital computer systems, that it is impossible to know whether the results produced by such a system are accurate, without some outside verification such as secured paper ballots, against which to check the results. It is precisely this possibility of auditability which computerized elections systems are designed to avoid. Even in the case of the optical scan systems, which do produce auditable paper ballots, procedures in use generally do not even involve spot checking or sample checking against the paper ballots, unless legal action is initiated.

Windows software, the internet, and the general laxness on such issues, make tampering with these systems easier than it might otherwise be, but the vulnerability is fundamental to the way that digital computers work. Unlike older mechanical counting systems, which also are not auditable, and can be rigged by the way the geared counting mechanisms are set up, computer systems can be programmed to use one set of software routines during testing, another during the election, and then wipe out either or both without a trace, so that later inspection, if it ever occurs, will make it appear like a third set was actually used in the election.

But, the special feature of elections systems, which renders all arguments for their security ludicrous, is this: Elections systems are not computers and software which are sold to and used by governments to conduct elections. The private elections systems companies actually control the election process! According to the Washington, DC Board of Elections and Ethics, Sequoia produces the software coding, with the ballot information and tabulation procedures for each election, burns that coding onto a memory cartridge, and installs it in the voting machines and the central tabulation machines. News reports and governmental studies reviewed, indicate that this is the general procedure followed for all computerized elections. Beyond that, it seems that, as in the case of the Diebold run year 2002 elections in Georgia, elections systems personnel are also generally on the scene to trouble-shoot problems, apply software fixes as necessary, and so on.

Computer security measures are generally designed to enable the proprietors of a system to protect it from outside tampering, including protecting the system by blocking certain functions even to most employees. Highly trusted operatives administer these controls to protect against less trusted operatives. No serious attention has ever been paid to protecting a computer system from those who design it and operate it, but, as the accompanying report on elections systems proprietors indicates, the most serious threat of tampering with these systems comes, not from outside hackers, but from the companies which design them and supervise their operation, with little or no interference from the government officials entrusted with the responsibility of running elections.

Proposed Remedies Can't Work

While potential problems with these computerized elections systems is generally admitted, the elections systems producers, and most governmental agencies involved, propose to avoid difficulties through various means.

In fact, the systems manufacturers themselves, have little to say in their own defense. In their July 20, 2003, published rebuttal to a team of computer scientists who identified vulnerabilities in their software, DIEBOLD's defense contained many words, but little substance beyond this introductory statement, “The Diebold AccuVote-TS touch screen voting station is just one element of the electoral process that is highly regimented and that has evolved and been honed over hundreds of years in the United States.”

Otherwise, they counter specific vulnerabilities with ideological statements such as, “To be true, this claim would require a {conspiracy} of unscrupulous voters or malevolent insiders, or a combination of the two. The electoral process is designed in such a way that no single individual, or even a small group of individuals, can tamper with the election results.” Nowhere do they point out that, in fact, DIEBOLD elections {are} run by a small group of individuals: the DIEBOLD technicians, who are the only people on the scene with any means of understanding what their machines are doing.

Now, we analyze each of the proposed control measures.

Certification of Software:

The National Association of State Election Directors (NASED), has established procedures for certifying elections systems equipment and software. This is a typical bureaucratic solution. If you can’t fix it, appoint an authoritative commission and declare that it’s fixed.

In reality, certification does nothing to plug the hole. As any computer professional knows, and as the constant need for refining “live” software attests, line by line reading of programs, which many propose as part of this procedure, and laboratory testing of software, does not guarantee adequate “live” functioning of the software. Since elections are always one-time events, requiring last minute programming or set up for the specific array of choices offered on the ballot for a given election, there is little opportunity for advance review and testing. Of course, it is precisely in this area--the set up for a particular election—where it is easiest to accidentally or deliberately change the results of an election by, for instance, simply having one candidate's votes counted for another.

In the Georgia case investigated extensively by Bev Harris (BlackBoxVoting.com), when bugs in the system were discovered while preparing for the election, Diebold did what one might expect: They by-passed all review and certification procedures and installed patches to fix the software on the spot.

Election Day Verification Testing:

Generally what is proposed is a specific list of testing procedures to guarantee the machines are functioning properly. In fact, codified testing procedures make it easier to design evasion of those procedures into the software. These pre-election procedures are like the magician's display of his equipment before his trick. As long as he follows his routine, and the audience looks where it's supposed to, the trick won't be discovered. I’ve witnessed these opening and closing election day ceremonies, but have never seen any opportunity for real scrutiny of the system. Unless the rules permit some ornery cuss, not a selected official, to interfere with the testers, re-run the tests as many times as he, not they, want, and, generally, try anything but the expected, these tests are meaningless.

Responsible Citizens, not Computers are Required

Without direct citizen involvement in the elections process, and full access to unbridled testing, ballot box security procedures, and so on, there is no way to guarantee fair elections. The computer systems proposed actually take control out of the hands of responsible officials and places it in the hands of private companies, most of which are heavily political in composition.

The most popular of these systems, the DRE's without audit trail, make the discovery of fraud or miscounting impossible, except by accident. Given the right kind of citizen activism, the best systems are the Optical Scanning systems, with the proviso that the paper ballots are actually secured and minimally spot-checked in normal circumstances, and recounted in the case of a legitimate dispute.