ELECTRONIC VOTING: AN OVERVIEW OF THE PROBLEM

David L. Dill
Professor of Computer Science, Stanford University
Founder of the Verified Voting Foundation and VerifiedVoting.org

Introduction

The winners of an election are usually satisfied with the outcome, but it is often more challenging to persuade the losers (and their supporters) that they lost. To that end, it is not sufficient that election results be accurate. The public must also *know* the results are accurate, which can only be achieved if conduct of the election is sufficiently transparent that candidates, the press, and the general public can satisfy themselves that no errors or cheating have occurred.

Unfortunately, the advent of paperless electronic voting (e-voting) is moving us away from election transparency. E-voting technology is extremely opaque. No one can scrutinize some of the most critical processes of the election, such as collection of ballots and counting of votes, because those processes will be conducted invisibly in electronic circuits. Voters have no means to confirm that that the machines have recorded their votes correctly, nor will they have any assurance of that their votes won't be changed later.

In the presidential election of 2004, almost 30% of American voters reportedly used e-voting machines, and this number is increasing because of the deadlines set by the Help America Vote Act, (HAVA) and the funding made available for new equipment by that law.

Accountability

The basic problems of e-voting can be understood without an in-depth knowledge of computer technology. A helpful analogy was proposed by computer security researchers Drew Dean and Dan Wallach: Suppose voters dictated their votes, privately and anonymously, to human scribes, and that the voters were prevented from inspecting the work of the scribes. Few would accept such a system, on simple common-sense grounds. Obviously, the scribes could accidentally or intentionally mis-record the votes with no consequences. Without accountability, a system is simply not trustworthy, whether or not computers are involved.

Are computers different in some important way from human scribes? Computers can execute programs accurately and with great speed, but they are designed and programmed by people who are no more reliable than our hypothetical scribes. Indeed, the construction of completely accurate and reliable hardware and software is one of the great unsolved problems of computer technology -- a problem that is actually growing worse with the burgeoning complexity of computer systems.

Computer systems can also be subverted intentionally. Most people are familiar with the "hacking" of systems by outsiders, often through the internet. Experience in computer security has shown that resisting such attacks is extremely difficult. The attackers are often very creative and determined, making them formidable adversaries. However, the greater threat to most systems is from *insiders*. Software can be modified maliciously by people with legitimate access before it is installed on thousands of individual voting machines. Indeed, much computer crime is perpetrated by insiders, because it is easier for them to commit crimes, and they are less likely to be caught. There is no reason we should be more trusting of insiders in the election industry than in other industries, such as gambling, where sophisticated insider fraud has occurred in spite of extraordinary measures taken to prevent it.

Many lay people assume that malicious software can somehow be detected by inspection or testing, but, perhaps surprisingly, there is no reliable way to do this. Computer systems are the most complex artifacts known; finding cleverly hidden malicious code is much harder than finding a needle in a haystack. (For some benign and fun examples of how easy it is to hide things in software, search for "Microsoft Easter Eggs" on the Internet.)

In the public debate, it may seem that there is some disagreement among technologists about the dangers of paperless e-voting, because the same two computer scientists opposing paper ballots speak at almost every forum. However, the overwhelming consensus of technical opinion is that e-voting is dangerous, and that voters need to be able to verify that their votes were properly recorded. The "Resolution on Electronic Voting", which I wrote in January 2003, has been endorsed many of the top researchers in computer science, including the authors of several of the most widely read texts on computer security. Also, the Association of Computing Machinery (ACM), the largest professional organization of computer technologists, has taken the position that "... voting systems should enable each voter to inspect a physical (e.g., paper) record to verify that his or her vote has been accurately cast and to serve as an independent check on the result produced and stored by the system." A poll was conducted on this question, and fully 95% of the respondent ACM members agreed with the statement.

Auditing and Paper Ballots

Systems are usually made trustworthy through independent checks, called "auditing." Secret ballots make voting uniquely difficult to audit. In other areas, such as finance and e-commerce, audit trails necessarily include the identities of the parties involved in transactions, but voting systems go to great lengths to destroy this information by design, as required by our system of secret ballots.

To understand how voting systems can be made auditable, let's return to the scribe analogy. One solution would be to eliminate the problematic scribe and have the voter fill out the ballot and deposit it in a ballot box. Or we could make the scribe accountable for his work by allowing the voter to inspect the ballot and deposit it in a secure ballot box (or watch the scribe do so). Analogous solutions will work for voting. We could simply use paper ballots marked by hand and counted by optical scanners; indeed, many U.S. voting jurisdictions use these systems, and have for decades, and the systems are highly accurate. Or "voter verifiable printers" could be attached to touch-screen machines to produce tangible ballots that voters could inspect.

Instead of attempting to solve the unsolvable problem of insuring the integrity of computer hardware and software, these measures place the responsibility on the voter to check that his or her ballot is filled out properly. Imperfections in the technology, whether from unreliable computers or unreliable pens, can be tolerated because each voter can check that his vote was handled properly. With these paper ballots, it is possible to do a meaningful manual count, for election auditing or in a recount, because the records being counted will be known to reflect the voters' intent.

This generic scheme has been described by various cumbersome phrases, such as "voter-verifiable paper audit trail" or "voter-verified paper ballots." Unfortunately, the awkward "voter-verified" modifier is necessary. A casual reading of HAVA has led many to conclude that it already requires voter-verified paper ballots, since it requires a "manual audit capacity." Unfortunately, this language is being interpreted to allow printing paper ballots from electronic memory after the close of the polls, for use in a manual recount. Of course, this interpretation renders the "manual audit capacity" nearly useless, because these paper records may not reflect the intent of the voters, who were unable to check the electronic records on which they are based. Hence, it is necessary to ensure that the voters are able to inspect the paper ballots before they are cast.

Paper ballots are not a magical guarantee of accurate and fraud-free elections. Indeed, there is a long history of errors and election fraud with paper ballots, but those problems stem from inadequate procedures, inadequate checks and balances, and inadequate auditing, not from the use of paper. Improving the trustworthiness of our elections will require attention to many other issues. If machines are used to count the ballots, they must be doubled-checked sufficiently using manual counts to detect and deter systematic fraud. The physical security of the paper ballots must be maintained from the time when they are marked by the voter until the last recount is complete. Above all, all aspects of the election must be open to public scrutiny, and the public must actually scrutinize the conduct of elections.

The conduct of elections in many places falls well short of these ideals. But the solution to that problem should be to improve those procedures, not to eliminate the evidence that could be used to detect errors or fraud. Using paperless electronic voting has been likened by Kim Alexander, President of the California Voter Foundation to "dealing with fraud by eliminating the accounting department." An ongoing nationwide effort to improve election practices is needed very badly.

These arguments against paperless e-voting are often dismissed on the grounds that "no election technology is perfect." While this is an undeniable truth, problems vary with different technology. Paperless e-voting is more dangerous than paper ballot systems because it opens the door to wholesale errors. A single bug, or malicious software installed by a single individual, could be distributed to thousands of machines around the country, which could then undetectably change a very large number of votes. And, contrary to the frequent assertions of vendors and some local election officials, there are *no* "checks and balances" that can reliably prevent or even detect these problems without paper ballots.

How did we get there?

The trend towards paperless e-voting has been driven by the laudable goals of enfranchising more voters and increasing the accuracy and integrity of the voting system. However, a crucial mistake was made, which was to make policy about computer technology without being informed about the limitations and hazards of that technology. Policymakers, without independent knowledge or advice about computer security, were assured by vendors and other proponents of the technology that it was safe, and did not inquire further.

Many claims are made of the superiority of e-voting, for example: the machines are more accurate, and allow users to correct mistakes; they are accessible to people with disabilities who cannot use paper or mechanical voting machines without assistance; they are easier for poll workers to use; and they save the cost of paper ballots.

Even taken at face value, these advantages would not justify sacrificing the transparency of our elections, but many of these claims turn out to be illusory when examined more closely. Studies have indeed shown that the best e-voting equipment is more accurate than the worst technologies, such as pre-scored punch cards, but most of the same studies show that precinct-based optical scan systems are actually more accurate than e-voting machines. (When using a precinct-based optical scan system, the voter fills out a paper ballot by hand and then places it in the optical scanner, which counts and stores the ballot. If there are too many votes for an office or a stray mark that prevents the ballot from being read properly, the scanner rejects it so the voter can correct the problem before casting a vote).

New equipment has recently become available to make it possible for voters with disabilities such as blindness to use optical scan ballots while voting privately; for example, there is a machine that allows voters to read and mark an optical scan ballot using a touch-screen or audio interface. Furthermore, while e-voting machines are accessible in theory, it is unknown how many voters with disabilities have been able to use them successfully in practice. The Silicon Valley Council of the Blind surveyed their members after a recent election only to discover that very few were able to use the new machines that had just been purchased in Santa Clara County, California.
(http://verifiedvoting.org/article.php?id=2102)

The claim that e-voting is easier for poll workers to deal with is implausible, and seems not to have been confirmed by experience. Dealing with a workplace full of computers is rarely easy in this day and age. Counties acquiring new e-voting equipment have had to implement extra measures to make sure there are technically capable poll workers (a difficult task) and to have technicians on call to deal with machine problems. Indeed, in recent elections many of the observed failures of e-voting equipment are blamed (often unjustly) on the inability of workers at the polling places to properly setup and operate the equipment.

Finally, e-voting machines cost at least three times as much as optical scan systems to purchase. Even ardent proponents of e-voting admit that this cost difference cannot be recouped in less than 15 years, which is greater than the lifetime of most computerized equipment. There is also some evidence that on-going costs for support and maintenance of e-voting equipment are higher than were estimated in many jurisdictions.

Where do we go from here?

A trustworthy election system depends on three factors: technology, procedures, and observation. Changes are needed in each of these areas. In many cases, election laws will need to be amended.

As was argued above, we need technology that allows each voter to verify that his or her vote was correctly captured. At this time, the only technology that can realistically meet this need is paper, because most voters can verify the contents without computer mediation (which is inherently untrustworthy), because it can be written indelibly, and because the procedures for protecting paper are understandable by ordinary poll workers and voters.

There are now several proposals for voter verification based on advanced cryptography. These systems are intriguing, but there are still many challenges to be met before they can be responsibly deployed in governmental elections. First, they are not widely understood even by computer science researchers, and have not yet been subjected to the in-depth scrutiny by independent experts that is necessary to be reasonably sure that a system is a secure. Indeed, some experts have commented that these schemes are much more complex than secure computer and communications equipment that has been certified for U.S. military and intelligence applications. Second, the operational and logistical details for using these schemes in real elections have not been worked out. Finally, and most importantly, these systems are completely non-transparent to the average voter, who cannot begin to understand how they work or why they should be trusted.

The second component of a trustworthy election is the use of appropriate procedures. If paper ballots are used, they have to be protected, and the processes for storing, transporting, handling, and counting them have to transparent. Ideally, members of the public and non-governmental organizations as well as political party representatives should be able to observe all of the steps of an election, including machine testing, polling place operations, counting of votes, auditing and recounting.

One of the most important reforms that could be adopted is routine auditing of elections by choosing a small random sample of the ballots, and manually counting them. Careful auditing should occur regardless of whether an election was close or whether there were apparent problems, results of the audit should be made public, and problems detected by the audit should be investigated. By adopting random manual audits universally, we can distinguish the idea of objectively checking an election, to reassure voters of its integrity, from recounts requested by candidates, which are often perceived as tactics for reversing an unwelcome election outcome. Audits are also a mechanism for election quality control. Routine audits will often catch problems in the conduct of elections that are not close, so they can be corrected before they cast the outcome of a closer election in doubt.

The final factor in trustworthy elections is independent observation. In too many states, election laws and practices do not allow independent observers to be present during crucial parts of the process, such as the testing of equipment. In others, only certified representatives of candidates or political parties may observe. This is fundamentally wrong. Elections exist first for the people, not for candidates and parties, and the people, the press, and representatives of non-governmental organizations must be allowed to observe. Finally, the public has an obligation to participate in elections, not only as candidates, but as poll workers and witnesses to the process. This participation should be encouraged by election officials as well as by independent organizations such as ours.

Fortunately, some of these reforms are already underway. Many people in the U.S. are belatedly recognizing that too many states and counties rushed into using e-voting in an overreaction to the problems in the 2000 presidential election. The issue is now drawing a great deal of attention. Many states have changed their plans to convert to e-voting, and now insist on paper ballots. At the Federal level, there are multiple bills in the House and Senate that would require voter-verified paper ballots.

Behind these developments is a large and effective grass-roots movement. The "paper trail movement" is unusual; it does not follow conventional partisan and ideological divides, and it has the participation of prominent computer science researchers, who have great expertise in the relevant areas of technology, and who rarely speak out on other policy issues. Last summer, more than 350,000 U.S. citizens submitted petitions demanding voter-verified paper ballots. This movement will continue to gain momentum, in part because increased attention to elections will expose more and more problems with the use of e-voting.

Conclusions

The recent controversy about electronic voting has focused attention on the conduct of elections, which had been neglected by the public and policymakers for far too long. Although this attention is uncomfortable for many in the elections community, it is healthy. Ultimately it will result in stronger foundations for our democracy.