Citizen's Guide to Voting Technology

Bruce O'Dell
Fortune 100 Computer Security Analyst and
Co-Producer of STEALING AMERICA: *Vote by Vote*

Excerpt. The entire article can be found at www.StealingAmericaTheMovie.com/GetActive

Q: There are a lot of academics and experts that say voting software is perfectly secure. What basis do you have for questioning their judgment?
A: I've made a career of helping my clients protect billions of dollars of other people's money from thieves, hackers and embezzlers, and I design very large-scale computer systems with extraordinary requirements for security and integrity. At American Express, I led a project to provide customer access to transactions from financial institutions throughout North America. I've served as the technical leader of a project to replace the access control software at one of the twenty biggest companies in America. And – unlike some of my academic and professional colleagues, who consult for or provide software to voting technology vendors or their clients – I have never had any financial interest in promoting e-voting technology.

Q: Why are you questioning the honesty of the people who create and program voting machines and who run our elections?
A: I'm not questioning anyone's honesty—but human nature is what human nature is. There's ample room for insider misconduct in any organization. Surprisingly enough, the most severe security risks in any organization are from insiders. Despite extraordinary security measures, banks and financial institutions continue to be ripped off by trusted insiders who understand exactly where the weaknesses are in the system. According to Dan Verton's recent book Identity Thieves, insiders accounted for approximately 70% of the $3.4 billion that banks lost to internal and external fraud and hacker incidents in 2004.

Q: What could possibly motivate so-called "malicious insiders" at the voting equipment companies to risk getting caught?
A: Our elections determine those leaders who command the world's only superpower military, set the agenda for federal law enforcement and who control the world's largest checkbook: our federal budget. By the "Willy Sutton" rule, voting systems are truly "where the money's at." Common sense tells me that constant, ruthless and highly sophisticated attempts by insiders to subvert voting software must be assumed to be currently underway, given such a valuable target.

Yet when it comes to voting systems, the presumption currently seems to be that attacks by malicious insiders are unthinkable. In the wake of a report of what was (at the time) "the worst security vulnerability ever found in a voting system," David Bear, a representative of Diebold Election Systems, was quoted as follows (New York Times, May 12, 2006):

> For there to be a problem here, you're basically assuming a premise where you have some evil and nefarious election officials who would sneak in and introduce a piece of software... I don't believe these evil elections people exist.

Imagine the reaction of a CEO or CFO upon hearing a company representative selling cash management software say that their clients do not need to worry about reports of a major security flaw in their software, because he doubted that any "evil bankers" existed. Heads would roll.

Q: Before it spun off its voting equipment division, Diebold manufactured both ATMs <u>and</u> electronic voting machines. Isn't casting your ballot on an electronic voting machine just as secure as taking cash from an ATM?
A: That's a common misconception – but in terms of security, ATM devices and electronic voting machines actually have almost nothing in common. It all comes down to one simple consideration: on the one hand, votes must be anonymous; while on the other hand, electronic financial transactions must be based on strong proof of identity.

Electronic financial transactions are as secure as they are – where embezzlement is the exception and not the rule – simply because you must first prove your identity to all the parties involved in any ATM transaction. Voting is an anonymous transaction. Electronic voting machines cannot apply to voting transactions any of the identity-based financial auditing mechanisms universally used by ATM machines. If they did, the secrecy of your ballot would disappear.

Q: I'm not sure I understand – can you give a concrete example why ATMs and electronic voting machines are so

different?
A: Just imagine what would happen if an election is run using e-voting equipment that applies the same security standards as banks do to ATMs. You sign on, enter your PIN number, and then cast your "ATM ballot." Your name is immediately sent to the computers owned by each candidate you vote for, and your name and ballot choices also go to your county and state election officials. You receive a printed receipt listing your ballot selections that is yours to take home with you. When the polls close, there's little doubt about who won the "ATM" election; every candidate would have a complete a list of all the voters who voted for him or her. You would even receive a statement from your county election office listing all your ballot choices as officially recorded. Since ATM-style security measures can't be applied in real world elections, voting by computer is extraordinarily risky.

Q: There's got to be some kind of process that election administrators use to double-check the accuracy of the voting machines after an election.
A: In contrast to banks that always audit all of their transactions, in the real world only a relative few states routinely audit any of their paper ballot records (if they still have any) to independently verify the accuracy of the machine tallies. Those few states that check their paper ballot records, only do so for a few percent of their precincts. If current "best practices" in American election administration were applied to the financial services industry – for example, if there were a bank that chose to independently audit only a few percent of its accounts, or simply trusted that its accounts were all accurate without any independent audit at all – its customers would flee in panic, regulators would shut it down, and its Board of Directors would face possible jail time.

Q: But you make it sound like there are no safeguards in place. Aren't voting machines certified by independent inspectors and subject to strict testing to make sure they are accurate?
A: The computer industry as a whole does not do a good job when it comes to building security into software products. But both practically and theoretically, it is impossible through testing to determine that any computer system has no flaws – much less, to rule out the existence of secret back-door functions to be triggered on a future date. After all, all computers have clocks and can tell time, and there are a vast number of ways to program them to behave differently when being tested than when deployed in the field during an election.

Q: How does the way Las Vegas protects electronic gambling equipment compare to how we protect electronic voting equipment?
A: Nevada performs elaborate, stringent and intrusive ongoing independent random inspections of the hardware and software of the actual electronic gambling equipment in use at all casinos. In stark contrast, the details of our electronic vote tallying systems are considered by their manufacturers to be "trade secrets" and as such are legally shielded from independent inspection. No voting system has ever been examined and tested in any jurisdiction in America with anything approaching comparable rigor, and if these manufacturers continue to have their way, none ever will. Despite all the stringent measures Nevada takes, insiders at the gaming equipment vendors and at the casinos have successfully compromised computerized gambling machines. Even though successful manipulation of election equipment yields far greater financial returns, those who suggest that electronic election manipulation by insiders is possibly underway are dismissed as "conspiracy theorists."

Q: But what if someone could inspect the voting machine software? Wouldn't an inspection of this kind find problems or even deter people from manipulating election equipment?
A: The source code is just a document. Source code, which is readable by humans, becomes translated into a "binary" version that is no longer human readable – but can be run by a computer. So I cannot tell simply by reading the official source code what binary logic is actually installed and running on any particular voting device in the field. "Source code inspection" actually misleads the public, making it seem as if IT professionals have superhuman powers to "know" what is actually running in a particular device in the field during an election – when of course, we do not.

Q: That's paranoid. Surely no one could ever subvert voting machines or voting software on a scale sufficient to change the outcome of elections without word leaking out? There must be many people involved in such an operation!
A: Actually, you wouldn't need very many people at all. Election administrators have hands-on access to memory cards and central tabulators. Even after the devices are tested in readiness for an upcoming election, local election officials have a surprising degree of cozy hands-on access to voting equipment. In fact, all over the country, voting machines are frequently brought home by poll workers for "storage" prior to the election. Voting equipment vendors allege that their equipment has tamper-proof seals, while in reality, it takes only minutes using household tools to gain sufficient access to voting equipment to permanently and in practice undetectably alter the software. Or, assume the employees at the voting equipment vendors are as trustworthy on average as the employees in any other corporation. All you would need is a small handful of people with the right level of access to the software distribution process. Alter the master copy of the software – any component, of

any of the software, from the operating system on up – and that change can eventually get copied to all the vendor's voting machines.

Q: Why do you really think that someone could – or even would – take such an enormous risk for uncertain results?
A: The risks are not so enormous, given the culture of American politics. As **STEALING AMERICA** reveals, voting systems are "presumed accurate" by politicians, the public and the media. Any electronic vote tallying system – even one with some kind of paper trail – is never fully audited unless a candidate challenges the result. If the official result is not particularly close, there is absolutely no political will to challenge it. In other words: the bolder, the better. And when recounts do occur, all too often, the fox is auditing the hen house with plenty of time to hide the bloody feathers.

For the first time in history, computerized election equipment has made possible an extraordinarily dangerous feedback loop. After all, you simply can't take down the American Republic by force of arms; a conventional violent coup won't work, but one with "manufactured consent" that appears to be reflecting the will of the people certainly will. An undetected series of gradually-increasing deceptive election results over time leads to the manufactured illusion of a shift in the underlying voting patterns of the electorate. Eventually, the manufactured reality becomes true insofar as we can perceive it. Exit polls and increasingly even the selection criteria for public opinion polls, are calibrated to "official" election results.

Q: Is there <u>any</u> kind of voting technology that can be made secure?
A: There was a remarkable article published by the Computer Professionals for Social Responsibility in 2001, citing work by the Caltech-MIT Voting Project, indicating that no form of voting technology ever invented is more accurate than people counting paper ballots, one at a time, by hand**.** If there is a superior alternative solution to any problem that does not involve computer automation, it is unethical for information technology professionals to advocate use of computers.

Q: But isn't it true that hand-counted paper ballots are just as vulnerable as machines, if not more so?
A: Paper-based processes are not perfectly secure, of course. But some of us certainly think we've figured out how to audit and safeguard paper-based systems, to an acceptable degree of public and commercial confidence, over the last few centuries. Here's a quick reality check: if you agree that it is impossible to effectively audit and safeguard paper, stop by your local bank and help yourself to the cash on the way out. Or if you're in Washington, drop in at the White House and pick up your own copy of the President's Daily Brief; I've heard it's fascinating reading.

The bizarre belief that it is impossible to run fair elections with hand-counted paper must come as a surprise to the citizens of Canada, New Zealand, Germany, Iraq... and so on, all of whom not only conduct their elections on paper, but also manage to double-check the outcome with an acceptable level of public satisfaction with the results. If you do not believe me, Google the phrase "Disputed Canadian Election."

Q: Don't we need computerized voting equipment to accommodate the needs of visually or mobility impaired voters?
A: You don't need computers to enable visually or mobility-impaired voters to cast ballots. For example, Wisconsin allows the use of the non-computerized VotePAD ballot marking device.

Q: But we've invested billions of dollars in advanced computerized voting technology. You can't seriously be suggesting we get rid of all of it?
A: I say technology professionals have an obligation to honestly advise the public whenever the most appropriate choice is not to use computers. Ireland and the Netherlands also recently purchased computerized voting equipment – and both countries are now throwing it all out in favor of a return to hand-counted paper ballots.

Q: Sure, hand counting paper ballots works in small countries, but isn't it impractical to count paper ballots by hand in a country as big as the U.S.?
A: The size of the country is irrelevant. A bigger country just means there are more counters working in parallel. The average American precinct has about 500 to 700 votes to count. Larger precincts can have multiple counting teams. This is hardly a problem that cries out for a computer.

Q: Do you really think the American people are up to the challenge? Almost half of us don't even bother to vote. Wouldn't the paper ballot process wind up just as bad or even worse than what we now have?
A: I, for one, don't believe that the people of countries like Canada, Ireland, Germany, Italy, the Netherlands (or Iraq, for that matter) have any special talents or civic virtues that enable them – but not us – to run elections on paper to a high level of public trust and confidence. I strongly believe that with the appropriate procedural checks and balances, we Americans can indeed gather together every couple of years and collectively count all the way up to 500 or so, several times, in public – without any computers to "help" us. I trust American citizens to safeguard the integrity of our Republic. .