Global Information Assurance Certification Paper

Trusting the Machine:

Inherent Problems with Electronic Voting Systems

I.V. Blankenship

GIAC Security Essentials Certification (GSEC)

Version 1.4b
Option 1

February 19, 2004

Table of Contents

Abstract

The Help America Vote Act of 2003 provided funding to states for the modernization of voting systems. This influx of money accelerated the purchase of new voting equipment, including Direct Recording Electronic (DRE) voting systems. As more information becomes available about the attributes of these systems to include strengths, weaknesses, and most importantly their vulnerabilities the greater the public outcry to change the way the systems operate in elections. This paper will cover a brief history of voting systems and then discuss the security problems inherent to DRE systems and the Federal Election Commission standards that are applied to electronic voting systems. Finally, this paper will provide options to help improve voter confidence in DRE systems.

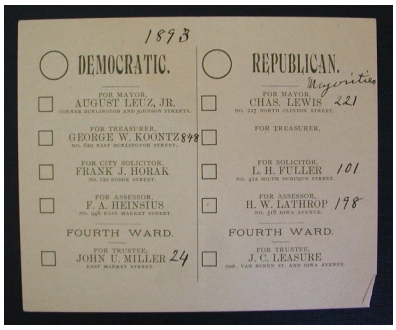
Introduction

In order for a democratic system to function voters must believe the entire election process from start to finish is fair. Even in the most contested elections, the group with fewer votes allows the group with the majority of the votes to take power peacefully. The system works because the electorate is confident that each vote is counted and every ballot possesses an intrinsic value. Throughout history, technological innovations have altered many aspects of life and raised people's expectations so that they demand more in less time. Elections are no exception. In the 2000 United States presidential election, the world was amazed that the outcome hinged on technology developed before humans walked on the moon. The amazement soon morphed into a demand to modernize the voting equipment used in throughout the nation. Legislation was passed and localities began to purchase modern electronic voting systems. In the rush to avoid another vote count scandal, systems were implemented that could potentially prove to be more corrosive to voter confidence than any number of chads.

A growing number of localities are adopting a new form of voting systems known as Direct Recording Electronic voting systems, or DRE for short. The new systems have not prevented controversy instead they spawn new issues and erode voter confidence. The new systems have failed in at least 15 states causing lost votes and since DRE systems stores all votes internally or in removable media there is no way to perform a recount of the data is suspect [Hol].

Voting System History

Paper ballots represent the oldest form of a voting system beyond a simple head count. First used in 139 BC by the Romans, paper ballots did not see use in the Americas until 1629 [Jon02]. Paper ballots made elections easier to run for large numbers of voters but did not prevent various forms of election fraud. The most notable form of fraud was ballot box "stuffing" where extra ballots are surreptitiously added in order to change the outcome of an election. Another form was the intimidation of voters made possible by the general lack of privacy when a person voted. In 1858 the Australians improved the paper ballot system [Jon02]. For the first time standardized ballots were printed at government expense, distributed to the voters at specified polling places where the voters must immediately complete the ballot in secret and return it to the election officials. The new system granted additional voter privacy and with a standard ballot format elections became less susceptible to fraud.


1893

DEMOCRATIC.

FOR MAYOR, AUGUST LEUZ, JR.

FOR TREASURER, GEORGE W. KOONTZ 848

FOR CITY SOLICITOR, FRANK J. HORAK

FOR ASSESSOR, F. A. HEINSIUS

FOURTH WARD.

FOR TRUSTEE, JOHN U. MILLER 24

REPUBLICAN.

Majorities

FOR MAYOR, CHAS. LEWIS 221

FOR TREASURER,

FOR SOLICITOR, L. H. FULLER 101

FOR ASSESSOR, H. W. LATHROP 198

FOURTH WARD.

FOR TRUSTEE, J. C. LEASURE

Illustration 1:Australian Ballot from an 1893 Iowa City municipal election [Jon01]

As with any adversarial system, a new counter measure gives birth to a new form of attack. Ballot tabulators were able to undermine elections utilizing secret Australian paper ballots as they evaluated marginal ballots that may or may not meet an established standard.

In this type of election rigging the party in power carefully selected counters that would zealously apply the standard to ballots that appeared to favor the opposition and relax the standard for ballots that favored their party [Jon02]. This form of election fraud and the complexity of the American general ballot were the number of candidates and initiatives vary by locality gave rise to a new voting system, lever voting machines.

First used in 1892, lever voting machines were hailed as a technical solution to the problem of counters manipulating ballot standards for political gain. A voter would enter the booth, select their choices, and pull the lever to record the vote. This system completely eliminated the problem of a biased counter and the machines could be configured to handle crowded election ballots. While one form of election rigging was exterminated, lever voting machines gave rise to other problems. The machines left no audit trail so there was no way to perform a recount. Also, the machines were expensive to test and maintain so localities were forced to trust the technicians who worked on the machines. If someone wanted to buy an election, all they needed to do was engage the services of a number of corrupt voting machine maintainers [Jon02].

As apparent as this vulnerability was, lever voting machines remained the standard in the United States until the middle of the 20th century when the Australian paper ballot made a come back with a high-tech enhancement. In 1964 IBM introduced the Votomatic punch card system with the goal of combining the strengths of the Australian secret ballot (voter privacy and a physical artifact for recounts) with the impartiality of machine tabulation. As the 2000 presidential election demonstrated, when the machine reading the cards fails to read the ballot it must be evaluated by humans thus opening the door to the same sort of manipulation that has plagued Australian ballots since their inception. Another problem with the punch card ballot is that it is difficult for the voter to verify that the hole punched in the ballot truly represents their choice. Without the ballot sleeve, voters are unable to match hole positions with candidates. Additionally, a poor ballot layout can cause confusion that may lead to a voter punching an unintended position. These problems were so serious that IBM ceased producing the Votomatic machines in the early 1970's and in 1988 the National Bureau of Standards recommended the immediate abandonment of punch card systems [Jon02]. Unfortunately, by that time the machines were the most common voting system in the United States with many localities occasionally dealing with the same problems that would manifest under an international spotlight in Florida 12 years later.

As the flaws in punch card systems were recognized in the 1970's, a new technology became available that address their weaknesses: optical mark sense ballots. This system does not require a special tool to mark the ballot (a simple pencil normally suffices), the voter can easily verify that their ballot reflects their intent, and a machine reader can be used to quickly tabulate the results. As with all paper ballot systems, the original ballots are available for recount in the case of a challenge, but this system is still susceptible to bias when the ballots are hand counted although they do have the lowest percentage of miscounted votes [Mer01 p. 50].

The newest class of voting machines is Direct Recording Election/Electronic (DRE) systems. These systems are essentially personal computers running specialized software. Just as punch cards and optical sense system are new twists on the Australian ballot, DRE systems are a high-tech version of lever machines. With touch screen interfaces, DRE systems reduce voter confusion, but as with the classic lever voting machines voters are forced to trust the machine vendors and the technicians who maintain the systems. While some DRE systems include a paper tape that records votes as they are cast, this is rare, so DRE voting systems generally do not provide a human countable record.

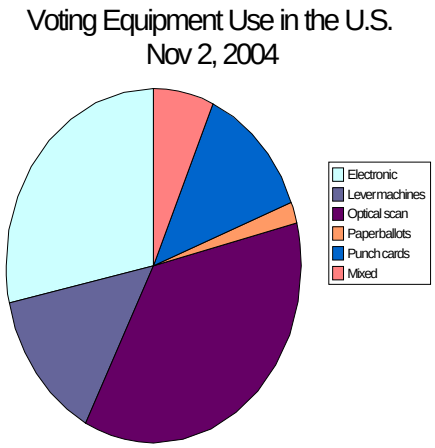


Illustration 2:Source: Election Data Services summary

Since there is no federal mandated voting system and the responsibility for organizing elections falls to individual localities there is currently a broad range of voting system used throughout the United States. According to Election Data Services, optical sense systems are the most common with 36 percent utilization followed by electronic systems at about 28 percent. Even after decades of use lever voting machines hold third place at 14 percent while punch card systems are used in just over 12 percent of the precincts in the United States [EDS].

The next type of voting systems will undoubtedly be a system where citizens are permitted to cast votes over the Internet. The first test of federally funded project named Secure Electronic Registration and Voting Experiment (SERVE) was slated to involve overseas voters in 50 countries and seven states. The test was canceled in February 2004 [Starr] after the release of a critical report citing numerous security flaws that could "easily allow a hacker to tamper with voting results" [CNN]. Privacy groups and members of academia including Dr. Rebecca Mercuri, a prominent computer security and electronic vote tabulation specialist, remain strongly opposed to Internet voting in any form. The main issue according to Dr. Mercuri is that the "voter has absolutely no control over the vote cast once it leaves his own computer system" [qtd Lan].

Election.com is a leading Internet voting company owned by Osan Ltd, a Saudi Arabian investment group, with Accenture (formerly Andersen Consulting of Arthur Andersen fame) holding the public sector assets [Lan]. This company has about 600 customers "including the Democratic National Committee, the Pennsylvania State Employees Credit Union, the Sierra Club, IEEE (The Institute of Electrical and Electronics Engineers, Inc.), the American Association for the Advancement of Science, the Florida Bar, and AIMR (Association of Investment Management and Research)" [Lan]. For many opponents of Internet voting, the possibility that public elections could be swayed by private companies owned or influenced by foreign nations or

companies that will benefit from a particular outcome of an election is more than enough justification to disallow public elections over the Internet. In order for democracy to function, the electorate must feel that contest was fair and trust every aspect of the election process.

Requirements for Secure Electronic Voting

Secure electronic voting implementations, through the use of Direct Recording Election (DRE) systems or over the Internet, should meet certain criteria before being trusted for use in elections for public office. Even as the nation prepares for the 2004 presidential election, bitter debates still rage about the results and procedures of the previous election. The controversy has generated intense public interest phasing out old punch card systems in favor of newer electronic systems. To this end, the Help America Vote Act (HAVA) of 2002 provides funding for states to replace punch card voting systems.

Peter Neumann of SRI International has suggested a basic set of standards by which an electronic voting system could be judged. The first criterion is system integrity where the "computer systems (in hardware and system software) must be tamper proof" [Neu] and subjected to rigorous configuration management. Once a baseline is approved, it must remain static with no last minute changes before an election. The system should not provide the capability to execute self modifying code and the initial operating system load be protected from the ability to install Trojan horses. In fact the "ability to install a Trojan horse in the system must be considered as a potential means of subverting an election" [Nue]. Most importantly the vote tabulation must result in "reproducibly correct results" [Nue].

Related to system integrity, is data integrity. For an electronic voting system it is imperative that each vote is recorded accurately and that once recorded, the data and the resultant tabulation are tamper proof. As the vote is recorded, the system should also ensure data confidentiality and voter anonymity. The results of a vote must not be readable externally and no association between the vote and voter made [Nue]. Additionally, all internal operations must be monitored without violating voter anonymity. This monitoring capability must be non-interruptible and impossible to circumvent with the resultant logs non tamperable.

As with any computer system, operator authentication is one of the most important security criteria. For electronic voting systems all personnel authorized to maintain the systems must gain access through "nontrivial authentication mechanisms" [Nue]. Fixed passwords or passwords that fail strict policies should be disallowed and between election cycles new strong passwords selected. Also there should be no trapdoors that permit "maintenance" access as this could provide a means to subvert the election machine.

Another criterion for a secure electronic voting system is disclosability. The electorate must trust that the election process is fair and that the process is transparent, the system software and hardware must be open for inspection. Also the "design, implementation, development practice, operational procedures, and testing procedures must all be unambiguously and

consistently documented" [Nue]. This documentation should be made publicly available to assure critics that the system is fair.

Two closely related security criteria are system availability and system reliability. The voting system must be hardened against intentional or accidental denial of service attacks and be available during the election process. The development process must strive to "minimize the likelihood of accidental system bugs and malicious code" [Nue].

The user interface presented to voters and election officials must be easy to use and be designed to prevent accidental and intentional misuse or improper configuration. Additionally, there should be no capabilities that permit any form of on-line operation from vendor technicians [Nue].

One of the most overlooked aspects of computer security is the personnel who will be using the systems. While much effort is invested in securing the system from external threats the developers and administrators of the system are often assumed to be harmless. More often than not, the truly damaging attacks come from within. For electronic voting systems the "people involved in developing, operating, and administering electronic voting systems must be of unquestioned integrity" [Nue]. Convicted felons, for example, should not be permitted to assist in the development, deployment, maintenance, or operation of electronic voting systems.

The criteria presented here are for the most part unattainable given current technology and the budgets localities are willing to spend on voting equipment. The criteria should be used to evaluate potential electronic voting systems and serve to illuminate the degree of insecurity for a given voting system. Systems based on commercial or proprietary products are normally closed to external review and may introduce a plethora of vulnerabilities if installed in a default configuration. A major flaw in direct recording election (DRE) systems is the absence of a physical vote record. Also in the case of DRE systems, external testing of the system is next to impossible with any degree of accuracy. For example a tester would have to cast several hundred ballots consistently never making a mistake and verify that the tabulation generated by the voting system is correct. In his testimony before the United States House of Representatives' Committee on Science, Douglass W. Jones admitted "We could not duplicate the human factors present at a real polling place in our tests, and we should trust the vendors and the labs to do that for us." [Jon02]

Shortcomings of Electronic Voting System Standards

In April 2002 the Federal Election Commission updated the 1990 Voting System Standards (VSS) to address issues and concerns that new electronic voting system introduced. While the new standards are an improvement there are still a number of shortcomings related to electronic voting systems. One of the most notable issues is the fact that third party commercial software is permitted for use in voting machines without a code review as long as the software is not modified. The VSS does not define a modification, but if any change from a default configuration, a security lockdown for example, counts as a modification then there may well exist voting systems with default

operating system installations. Default installations are notorious for lax security settings to include default passwords and excessive file permissions and user privileges.

Another obvious problem involved with the use of third party commercial software, or Commercial Off the Shelf (COTS), is that they introduce vulnerabilities (some well known) or instability into the voting system that could potentially be exploited by malicious voters, election workers, or even the vendor. The VSS makes no recommendations for approved operating systems or software and does not specify any standards for a secure configuration.

Additionally, COTS software is generally designed to operate on commodity hardware. High ability features in both hard ware and software are difficult and expensive to implement. DRE systems tend to be composed of inexpensive hardware potentially running on operating system with a reboot being the singular corrective action. In the Florida 2002 election, 100,000 votes were reportedly lost due to software error [Hol].

Changes to the commercial software may impact the operation and security of voting system. Douglass W. Jones discovered an example of this effect while testing DRE systems:

> "We found an interesting and obscure failing that was directly due to a combination of this exemption and a recent upgrade to the version of Windows being used by the vendor in their machine. In effect, the machine always subtly but reliably revealed the previous voter's vote to the next voter using the same machine! This was because, whenever a particular set of "pushbuttons" was displayed on the screen, the button most recently pressed was shown with slightly different shading. Such a set of buttons is frequently referred to as a *radio button widget*. As far as the developers of Windows were concerned, this new feature of radio button widgets was intended to help computer users remember what they'd done the last time they encountered a particular menu on their computer screen" [Jon02].

Another issue with allowing the use of commercial software without review in voting systems is the potential for even a slight appearance of favoritism on the part of the vendor. Consider the past adversarial relationships between companies such as IBM and more recently Microsoft with the federal government. In the Microsoft case, the candidate Bush was opposed to the antitrust litigation and Microsoft hoped to "delay hearings on their antitrust case until after the election" [Jon02]. In this case, Microsoft would benefit from a particular outcome of an election.

In section 6.5.3 the Voting System Standards specify that data from electronic voting systems be protected by the implementation of "an encryption standard currently documented and validated for use by an agency of the U.S. Federal Government " [FEC]. This is a very broad statement that does little to specify a minimum level of protection. Notably absent is a mention of key management policies. Without the specification of a strict key management system a vendor could use the same encryption key on every voting machine that they produce. Another shortcoming of the standard is the lack of a

specified digital signature standard. The VSS simply mandates the use of a "standard transmission error detection and correction methods such as checksums or message digest hashes" [FEC]. The focus of the standard appears to be error correction as opposed to authenticity. Authenticity is vitally important in the case of Internet voting were the voter must be sure that the ballot presented is correct or in the case of DRE systems that store an image of a ballot.

The most troubling shortcoming of the new Voting System Standards is the failure to require DRE systems to produce a voter verifiable ballot or a human readable audit trail. Everything is stored in media attached to the voting machine, should a machine be compromised then all the votes cast on that machine are be suspect. An important part of the post election process is the "ability of third-parties (such as press agencies, the League of Women Voters, and research organizations) to independently re-verify the election from the materials that voters actually used" [Mer02]. Without these safeguards voters should have little confidence that they vote they cast is actually counted.

The Mercuri Method

A solution to the lack of voter verifiable output for DRE voting systems is the Mercuri Method. Dr. Rebecca Mercuri has proposed a system that has all the benefits of a DRE system (ease of use, accessibility for impaired voters, rapid tabulation, etc.) yet still produces a human readable artifact for voter verification and recounts in the case of a challenge by one or more parties. With the Mercuri Method a voter enters a booth and makes their selections on the DRE interface. The system then prints a human readable paper ballot inside a sealed transparent chamber. The separation prevents the voter from removing the ballot from the polling place and protects the ballot from accidental of intentional modification. The voter inspects the ballot for correctness and then it is deposited mechanically into a ballot box while the DRE records the ballot internally. If the ballot was not correct then the voter asks an election official to void the ballot and permit the voter to try again. Once the election is over, the DRE totals serve as the preliminary results until the paper ballots are scanned and tabulated [Mer01].

The Mercuri Method is also cost effective in the long run since elections no longer require blank ballots printed before each election. As an additional security measure each ballots can be digital signed with a cryptographic hash composed of information such as a precinct code, the voting machine serial number, and a choices on the ballot. The hash would provide an extra layer of verification to help determine if a set of ballots were tampered with before they were counted without violating voter privacy.

While the method improves voter confidence and provides an audit trail, it does not prevent election fraud if the DRE is subverted. An election could still be rigged if the DRE randomly altered perhaps one ballot in 100. If a voter checked the ballot and noticed the change they would probably assume they entered the wrong choice. If they did not bother to check then the altered ballot would be counted as correct. Such and attack would be sufficient to swing close elections if applied in critical precincts.

Open Source Alternative

The use of closed proprietary software in DRE voting systems has generated a great deal of mistrust as vocal groups make the systems' flaws public knowledge on the Internet. Much of the criticism would be quelled if the concerned groups had the ability to review the code. The Open Voting Consortium is currently developing a prototype of free software licensed under the GNU Public License. Designed to run on inexpensive PC hardware, the project will provide verified voter ballots and provide multi-lingual support in addition to support for disabled voters. According to the OVC web page, the project hopes to have a demonstration version in February 2004.

The Voter Confidence Acts

In response to the growing resistance to DRE systems that do not provide voter verifiable ballots Representative Rush Holt of New Jersey "introduced a bill that would require a voter-verifiable audit trail on every voting system" [VV]. The bill is H.R. 2239 and in addition to requiring verifiable ballots the bill also bans the use of undisclosed software and wireless communications devices. Senator Robert Grahm introduced an identical companion bill, S. 1980) into the Senate in December 2003. At this time both bills are in committee awaiting further co-sponsorship.

Summary

Democracy can only function so long as the electorate has confidence that their vote matters. One of the results of the controversial 2000 presidential race was the acceleration of the process to modernize election systems. Unfortunately, election standards have not kept up with the changing technology and as a result many electronic voting systems, Direct Recording Electronic (DRE) systems in particular, are certified but raise serious questions about security, accuracy, and reliability. The software running on DRE systems is exempt from public review in order to maintain vendor trade secrecy. Also, third party software such as the operation system that runs voting system is exempt from review.

The Federal Election Commission (FEC) Voting System Standards (VSS) loosely defines encryption standards for use in DRE voting systems but does not specify a minimum policy for key management. Also while error correction checksum and hashes are mentioned, a standard for ensuring authenticity is not specified.

DRE systems are not required to produce a human readable ballot for voter verification. As a result, when a person votes on a DRE system they have no guarantee that their vote was registered or that the vote was not changed before it was counted. Another implication of the absence of a paper audit trail is that ballot recounts by the press or private groups is not possible.

The Mercuri Method is a proposed system to add voter verification to DRE systems by the production of a paper ballot printed from the voting system. The paper ballot counts as the official record and provides a human readable audit trail. There are currently bills in both houses of the United States

Congress to make voter verification a requirement on all Direct Recording Electronic systems.

References

[CNN] CNN, Daniel Sieberg and Alex Walker contributing. “Federal remote voting system called flawed.” Jan 22, 2004. URL:http://www.cnn.com/2004/TECH/01/21/internet.voting/ (Feb 2004)

[EDS] Election Data Services, “Voting Equipment Summary By Type as of 11/02/2004.” Feb 10, 2004. URL: http://www.electiondataservices.com/votingequipmentsummarybytype2004.pdf (Feb 2004)

[FEC] Federal Election Commission. “Voting System Standards.” Apr 30, 2002. URL:http://www.fec.gov/pages/vssfinal/vss.html (Feb 2004)

[Hol] Holt, Rush. “Rep. Rush Holt Introduces Legislation to Require All Voting Machines To Produce A Voter-Verified Paper Trail.” May 22, 2003 URL: http://holt.house.gov/issues2.cfm?id=5996(Feb 2004)

[Jon01] Jones, Douglas W. “A Brief Illustrated History of Voting.” URL: http://www.cs.uiowa.edu/~jones/voting/pictures/ (Feb. 2004)

[Jon02] Jones, Douglas W. “Problems with Voting Systems and the Applicable Standards.” May 22,2001. URL:http://www.cs.uiowa.edu/~jones/voting/congress.html (Feb 2004)

[Lan] Landes, Lynn. “Internet Voting - The End of Democracy?” Aug 27, 2003. URL: http://www.ecotalk.org/InternetVoting.htm (Feb. 2004)

[Mer01] Mercuri, Rebecca. “A Better Ballot Box?” IEEE Spectrum. Oct 2002: 46 – 50.

[Mer02] Mercuri, Rebecca. “Comment on FEC VSS Draft Volume 1.” Sep 10, 2001. URL:http://www.notablesoftware.com/Papers/FECRM.html (Feb. 2004)

[Neu] Neuman, Peter G. “Security Criteria for Electronic Voting.” Sep 1993 URL:http://www.csl.sri.com/users/neumann/ncs93.html (Feb 2004)

[Starr] Starr, Barbara. “Pentagon halts Internet voting System.” Feb 5, 2004. URL:http://www.cnn.com/2004/ALLPOLITICS/02/05/elec04.prez.internet.voting/index.html (Feb 2004)

[VV] Verified Voting. “Campaign To Demand Verifiable Election Results.” URL:http://www.verifiedvoting.org/fair_elections.asp (Feb 2004)