Kurt Williams
CS305
3/1/09

E-Voting Threatens American Democracy

Introduction

E-voting in the United States started in 1987 but has gathered steam rapidly in the last few years. It is now used by about a third of voters. Current e-voting systems use proprietary software for recording and counting the votes. The purpose of this paper is to convince the reader that the proprietary nature of the software, along with lack of security and the absence of a paper record threatens the integrity of our democracy. I will focus attention primarily on the Direct Recording Electronic voting systems (DRE) since I believe that they are the most dangerous.

History

Although the first commercially successful DRE system was patented in 1987, they were not widely used in governmental elections until after 2000. The controversy churned up by the close and contentious 2000 presidential election focused the nation's attention on its troubled voting system. In 2002, the Help America Vote Act was passed, providing nearly four billion dollars to replace punch card systems with DRE or optical scan systems and mandating that every polling place have at least one disabled accessible voting device. In the 2006 election, 38.4% of voters used DRE systems to cast their votes.[7]

Motivation

The Motives for implementing e-voting are good ones. Punch card ballots are problematic. We all remember the infamous hanging chad from the 2000 presidential election. Many votes were not counted because punch cards were flawed or improperly used. Optical scan ballots are better but can be confusing to the voter. Both punch cards and optical scan ballots can be difficult or impossible for disabled people to use. Additionally, considering that 170 million people were registered to vote in the United States in 2008, both systems require a lot of paper ballots that must be printed and stored at considerable expense. DRE systems could solve those problems. They can have the most accessible interface that we can invent, they can store votes electronically, and they can report the results to us at the end of the election.

Problems

As it turns out, DRE systems have a few problems of their own. These problems have generated a bit of controversy in recent years. In 2004, a system made by Unilect lost 4438 votes due to a memory issue in an election in North Carolina.[7] Also, in the 2000 presidential election, a Florida county recorded -16022 votes for Gore and 2813 votes for Bush in a precinct with only 600 registered voters.[8] In general, computerized voting adds complexity to and increases the number of points of failure in the election system. Problems can be categorized into three main areas: lack of transparency, lack of security and lack of verifiability.

Transparency

Without transparency, there is no way to know if the software is buggy or intended to fraudulently record/count votes. Proprietary software are considered trade secrets and as such are protected by law. A company cannot be compelled to publish their source and consequently independent parties have difficulty verifying the quality and honesty of the code.

After some discrepancies encountered in Union County NJ, the county asked Edward Felten, a Princeton computer science professor to conduct an independent examination of the systems. Sequoia, the manufacturer, informed the county that this would violate the license agreement and threatened legal action. The independent examination was subsequently canceled. In this case, the importance of an election's integrity was superseded by Sequoia's trade secret protection.[2] Opponents of publishing source code contend that concealing the source provides a measure of security.

Security

Without security, we cannot be confident that the software being used is the software that was certified or that the system has not been hacked. We have only to look at the numerous viruses, worms and trojan horses that have circulated recently to recognize that software security is not easily attained.

Hardware security is also an issue. The Diebold TS machine has a switch on the main-board that allows the systems to be configured to boot from EPROM, flash memory or external flash memory. This vulnerability would allow malicious software to be installed by anyone with a moment's access to the machine.[5] Also, only New York and Minnesota currently ban wireless components on voting machines.

Wireless access would make these machines vulnerable to being hacked remotely and invisibly.

In fact, the products of all three major e-voting vendors (Diebold, Sequoia and Hart Intercivic) have been demonstrated to have numerous and severe security failures. The Sequoia system's firmware can be overwritten using malicious files or an update cartridge. Security specialists were able to hack into a Diebold system and upload drivers that enabled the use of wireless components plugged into the back of the machine. The specialists were also able to change user permissions to allow a voter to perform actions reserved for poll workers or administrators.

What is worse is that Diebold appeared to have been aware of at least some of these security holes. An email from a Diebold programmer uncovered in 2001 stated: “Our smart-card format has absolutely no security, so if someone were to get a copy of this software and a reader, they could stand at the ballot station and quietly burn new voters cards all day”.[5]

Hart systems use a custom operating system that evaluators were able to circumvent and boot the system in a standard Windows environment before running the voting software. The testers were able to further exploit this system using an undisclosed user account that resulted in unauthorized and unhindered access to the system.[6]

Verifiability

Without verifiability, there is no way to know that a vote was counted the way the voter intended. Given the security vulnerabilities mentioned above and the expectation that there will be no perfect solution: verifiability is of particular importance. Since there is no paper ballot that will be counted, there is no means by which a voter can confirm that their vote was recorded correctly. It is also important to note that this verification cannot be done after the voter leaves the booth as this would compromise anonymity. If an e-voting system produces a paper audit trail, this would only be of value if the voter verifies the record before leaving.

Alternatives

Instead of DRE systems we could continue to use optical scan systems for most voters and provide another means of voting for disabled people. We could also use electronic ballot markers. Electronic ballot markers are e-voting systems that have an electronic user interface, but produce a printed paper ballot that the voter subsequently places into a ballot box.

Electronic ballot markers provide voters with a human readable ballot that they can verify and a paper record that can be used to confirm the results of the election. The ballots are machine readable and human readable, so they can be counted automatically or manually. They have the tremendous benefit of making errors evident. If a voter casts her ballot for candidate A and the machine prints a ballot for candidate B, this will be easily observed by the voter. This does assume, however, that the voter will examine the ballot. Critics claims that most voters will not verify their ballots. This may be true, but even one in five hundred voters might be enough to identify problems with voting systems. Opponents of this kind of system also argue that the cost of printing and storing all these ballots is too much.

My Opinion

The integrity of our election system is far too important to risk for reasons of cost or convenience. If we are willing to spend almost a trillion dollars bailing out banks to prevent our economy from collapsing, it is not unreasonable to expect that we would incur some significant cost to prevent our democracy from being compromised.

Also, the need for transparency must take precedence over trade secret protection. If I make the voting machines and I do not have to show anyone my code, then rigging an election is relatively easy to do. Any vendor unwilling to publish its source code must be considered unqualified for use in governmental elections. Source code must be made available to everyone. Security through obscurity is a fallacy. One has only to look at the countless security problems with popular proprietary operating systems to recognize this. In fact, problems with the Diebold TS were first uncovered due to source code leaked to the Internet.[5]

Additionally, we should fully expect election fraud. The incentives to steal an election are simply enormous. Think about what is at stake in a United States presidential election: The winner gains unfathomable political influence, assumes leadership of a nation with a fourteen trillion dollar economy and takes control of possibly the most powerful military in human history. Even with a generous view of human beings, one must concede that someone out there will be willing to cheat to acquire that kind of power. To conclude anything else would be foolish.

Consequently, electronic ballot markers and optical scan systems that produce a voter verified paper ballot are the only acceptable e-voting systems. Even with these, rigorous steps must be taken to secure them and transparency must be maintained.

References

1. Adayoshi Kohno, Adam StubbleField, Aviel D. Rubin, Dan S. Wallach. Analysis of an Electronic Voting System. IEEE Symposium on Security and Privacy 2004. ://avirubin.com/vote.pdf
2. Bosavage, Jennifer. New Jersey Clerks Want Sequoia E-Voting Investigated. 2008. http://www.crn.com/government/206905445
3. Brennan Center For Justice. 2006. Brennan Center Task Force Says Software Attacks Pose Real Danger to All Electronic Voting Machines. http://www.brennancenter.org/content/resource/brennan_center_task_force_says_software_attacks_pose_real_danger_to_all_ele/
4. Dechert, Alan. WORST EVER SECURITY FLAW FOUND IN DIEBOLD TS VOTING MACHINE. ://www.openvotingfoundation.org/tiki-read_article.php?articleId=1
5. Gimbel, Barney. Rage against the machine. Fortune Magazine. November 3 2006. ://money.cnn.com/magazines/fortune/fortune_archive/2006/11/13/8393084/index.htm
6. McCullagh, Declan. Sequoia warns Princeton professors over e-voting analysis. ://news.cnet.com/8301-13578_3-9897597-38.html
7. Morphy, Erika. Study: Hackers Could Change E-Voting Machine Results.2007. http://www.technewsworld.com/story/58572.html?wlc=1236579559
8. ProCon.org. Historical Timeline, Electronic Voting Machines and Related Voting Technology. ://votingmachines.procon.org/viewresource.asp?resourceID=273
9. Thompson, Alistair. Diebold Memos Disclose Florida 2000 E-Voting Fraud. 2003. ://www.scoop.co.nz/stories/HL0310/S00211.htm
10. Zetter, Kim. National: E-voting: No Fix Yet. 2006. http://www.verifiedvotingfoundation.org/article.php?id=6394