WRITTEN TESTIMONY OF DAVID WAGNER, PH.D.
COMPUTER SCIENCE DIVISION
UNIVERSITY OF CALIFORNIA, BERKELEY
BEFORE THE COMMITTEE ON SCIENCE AND COMMITTEE ON HOUSE ADMINISTRATION
U.S. HOUSE OF REPRESENTATIVES
JULY 19, 2006

Thank you for the opportunity to testify today. My name is David Wagner. I am an associate professor of computer science at U.C. Berkeley. My area of expertise is in computer security and the security of electronic voting. I have an A.B. (1995, Mathematics) from Princeton University and a Ph.D. (2000, Computer Science) from U.C. Berkeley. I have published two books and over 90 peer-reviewed scientific papers. In past work, I have analyzed the security of cellphones, web browsers, wireless networks, and other kinds of widely used information technology. I am a member of the ACCURATE center, a multi-institution, interdisciplinary academic research project funded by the National Science Foundation[1] to conduct novel scientific research on improving election technology. I am a member of the California Secretary of State's Voting Systems Technology Assessment Advisory Board[2].

Background

Today, the state of electronic voting security is not good. Many of today's electronic voting machines have security problems. The ones at greatest risk are the paperless voting machines. These machines are vulnerable to attack: a single person with insider access and some technical knowledge could switch votes, perhaps undetected, and potentially swing an election. With this technology, we cannot be certain that our elections have not been corrupted.

Studies have found that there are effective security measures available to protect election integrity, but many states have not implemented these measures. The most effective defense involves adoption of voter-verified paper records and mandatory manual audits of these records, but only 13 states have mandated use of these security measures. (At present, 27 states mandate voter-verified paper records, another 8 states use voter-verified paper records throughout the state even though it is not required by law, and the remaining 15 states do not consistently use voter-verified paper records. Of the 35 states that do use voter-verified paper records statewide, only 13 require routine manual audits of those records[1].) Voter-verified paper records provide an independent way of reconstructing the voter's intent, even if the voting software is faulty or corrupt, making them a powerful tool for reliability and security.

Problems

The federal qualification process is not working. Federal standards call for voting machines to be tested by Independent Testing Authorities (ITAs) before the machines are approved for use, but the past few years have exposed shortcomings in the testing process. The ITAs are approving machines with reliability, security, and accuracy problems. In the past several years:

[1]This work was supported by the National Science Foundation under Grant No. CNS-052431 (ACCURATE). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

[2]I do not speak for UC Berkeley, ACCURATE, the California Secretary of State, or any other organization. Affiliations are provided for identification purposes only.

- ITA-approved voting machines have lost thousands of votes. In Carteret County, NC, voting machines irretrievably lost 4,400 votes during the 2004 election. The votes were never recovered[2]. In 2002, vote-counting software in Broward County, Florida, initially mis-tallied thousands of votes, due to flaws in handling more than 32,000 votes; fortunately, alert election officials noticed the problem and were able to work around the flaws in the machines. In 2004, the same problem happened again in Broward County, changing the outcome on one state proposition[3] [4], and in Orange County[5]. In Tarrant County, Texas, an ITA-approved voting system counted 100,000 votes that were never cast by voters[6].

- ITA-approved machines have suffered from reliability flaws that could have disrupted elections. California's reliability testing found that one ITA-approved voting system suffered from mechanical and software reliability problems so severe that, if it had been used in a real election, about 20% of machines would have experienced at least one failure during election day and probably would have had to be taken out of service[7].

- ITA-approved machines have been found to contain numerous security defects that threaten the integrity of our elections. Over the past several years, we have been inundated with revelations of security flaws in our voting systems from academics (e.g., Johns Hopkins University, Rice University[8]), industry consultants hired by election administrators (e.g., SAIC[9], Compuware[10], InfoSENTRY[11], and RABA[12]), and interested outsiders (e.g., Finnish researcher Harri Hursti[13] [14]). None of these flaws were caught by ITAs. In the past five years, at least eight studies have evaluated the security of commercial voting systems, and every one found new, previously unknown security flaws in systems that had been approved by the ITAs. In my own research, I was commissioned by the State of California to examine the voting software from one major vendor, and I found multiple security flaws even though the software was previously approved by ITAs[15]. One of these flaws was discovered at least three times by independent security experts over a period of nine years (once in 1997, again in 2003, and again in 2006), but was never flagged by the ITAs at any point over that nine-year period[16].

All of these defects were ostensibly prohibited by federal standards[17], but the ITA testing and federal qualification process failed to weed out these problematic voting systems. The consequence of these problems is that the federal qualification process is at present unable to assure that voting systems meet minimum quality standards for security, reliability, and accuracy.

Federal standards have so far failed to address these problems. The 2005 VVSG standards do not remedy the demonstrated failures of the process to screen out insecure, unreliable, and inaccurate machines.

These failures have exposed structural problems in the federal qualification process:

- The ITAs are paid by the vendors whose systems they are evaluating. Thus, the ITAs are subject to conflicts of interest that raise questions about their ability to effectively safeguard the public interest.

- The process lacks transparency, rendering effective public oversight difficult or impossible. ITA reports are proprietary—they are considered the property of the vendor—and not open to public inspection. Also, if a voting system fails the ITA's tests, that fact is revealed only to the manufacturer of that voting system. In one widely publicized incident, one Secretary of State asked an ITA whether it had approved a particular voting system submitted to the ITA. The ITA refused to comply: it declined to discuss its tests with anyone other than the voting system manufacturer, citing its policy of confidentiality[18].

In addition, the secretive nature of the elections industry prevents independent security experts from performing their own analysis of the system. Technical information about voting systems is often considered proprietary and secret by vendors, and voting system source code is generally not available to independent experts. In the rare cases where independent experts have been able to gain access to source code, they have discovered reliability and security problems.

- Testing is too lax to ensure the machines are secure, reliable, and trustworthy. The federal standards require only superficial testing for security and reliability. For instance, California's tests have revealed unexpected reliability problems in several voting systems previously approved by ITAs. In my opinion, California's reliability testing methodology is superior to that mandated in the federal standards, because California tests voting equipment at a large scale and under conditions designed to simulate a real election.

- Many standards in the requirements are not tested and not enforced. The federal standards specify many requirements that voting systems must meet, and specify a testing methodology for ITAs to use, but many of the requirements are not covered by that testing methodology. The ITAs only apply whatever tests are mandated by the standards. The consequence is that the federal standards contain many requirements with no teeth. For instance, Section 6.4.2 of the 2002 standards requires voting systems to "deploy protection against the many forms of threats to which they may be exposed"; the security vulnerabilities listed above appear to violate this untested requirement. Likewise, Section 6.2 requires access controls to prevent "modification of compiled or interpreted code"; three of the major vulnerabilities revealed in the past two years have violated this requirement. These requirements appear to be ignored during ITA testing and thus have little or no force in practice.

- Parts of the voting software are exempt from inspection, reducing the effectiveness of the federal testing. The federal standards contain a loophole that renders Commercial Off-the-Shelf (COTS) software exempt from some of the testing. The COTS loophole means that the security, reliability, and correctness of those software components are not adequately examined. COTS software can harbor serious defects, but these defects might not be discovered by the federal qualification process as it currently stands.

- Even if an ITA finds a serious security flaw in a voting system, they are not required to report that flaw if the flaw does not violate the VVSG standards. Thus, it is possible to imagine a scenario where an ITA finds a flaw that could endanger elections, but where the ITA is unable to share its findings with anyone other than the vendor who built the flawed system. Relying upon vendors to disclose flaws in their own products is unsatisfactory.

- There are disincentives for local election officials to apply further scrutiny to these machines. Some local election officials who have attempted to make up for the gaps in the federal qualification process by performing their own independent security tests have faced substantial resistance. After one Florida county election official invited outside experts to test the security of his voting equipment and revealed that the tests had uncovered security defects in the equipment, each of the three voting system vendors certified in Florida responded by declining to do business with his county[19]. The impasse was resolved only when the State of Florida interceded[20]. In Utah, one election official was pressured to resign after he invited independent security experts to examine the security of his equipment and the testing revealed security

vulnerabilities[21] [22]. The barriers to performing independent security testing at the local level heighten the impact of shortcomings in the federal standards.

- If serious flaws are discovered in a voting system after it has been approved, there is no mechanism to de-certify the flawed system and revoke its status as a federally qualified voting system.

The 2005 VVSG standards do not address these structural problems in the federal qualification process. The 2005 VVSG standards were drafted over a period of approximately three months. With such an extremely constrained time schedule, it is not surprising that the 2005 standards were unable to satisfactorily address the fundamental issues raised above.

The shortcomings of the 2005 VVSG standards have several consequences:

- We are likely to continue to see new security and reliability problems discovered periodically. The security and reliability of federally approved systems will continue to be subject to criticism.

- Shortcomings at the federal level place a heavy burden on states. The 2005 VVSG standards do not provide enough information about the reliability and security of these machines to help states and counties make informed purchasing decisions. This places an undue burden on local election officials. Some states are doing their best to make up for gaps in the federal process, but many states do not have the resources to do so.

  Also, the increased scrutiny at the state level has the potential to subject vendors to dozens of involved state-level certification processes that have been instituted to make up for the gaps in the federal process, increasing the compliance burden on vendors.

- Millions of voters will continue to vote on voting machines that cannot be independently audited. This may diminish confidence in election results. In the event of any dispute over the outcome of the election, it may be impossible to demonstrate whether the election was accurate. Allegations of fraud may be difficult or impossible to rebut, due to the fact that today's paperless voting machines do not generate and retain the evidence that would be required to perform an effective audit. The lack of openness and transparency regarding voting system source code, testing, and equipment may spawn further distrust in voting systems.

- Voting equipment may still be subject to security and reliability problems, even if they comply with the 2005 VVSG standards. Many of the security and reliability defects described above would not have been prevented even if the 2005 VVSG standards had been in force when the machines were evaluated. Approval under the 2005 VVSG standards is not a guarantee of security or reliability.

Recommendations

The Technical Guidelines Development Committee (TGDC) and the Election Assistance Commission (EAC) could improve the VVSG standards and begin to address these shortcomings by taking several steps:

- Mandate voter-verified paper records and mandatory manual audits. Stop approving paperless voting machines. Today's paperless voting machines are not auditable. There is no effective way to independently check whether their results are accurate or to detect electronic

fraud. The inability to audit these machines greatly heightens the impact of security problems. Ensuring that election results can be independently audited would go a long way to reducing the impact of security defects in voting equipment. The 2007 VVSG should mandate voter-verified paper records and automatic manual audits of those records after every election.

- Broaden the focus beyond functionality testing, and embrace discipline-specific methods of testing voting equipment. Today, the standards primarily focus on functionality testing, which evaluates whether the machines implement all necessary functionality. Standards need to be expanded to incorporate technical evaluations of the security, reliability, and usability of these machines. The standards must incorporate the different forms of evaluation these disciplines each require. For instance, security evaluation is unique, in that it must deal with an active, intelligent adversary; functionality concerns the presence of desired behavior, while security concerns the absence of undesired behavior. Consequently, system security evaluations should always include an adversarial analysis, including a threat assessment and a source code review. The testing methods in the standard should be updated to reflect the state of the art in each discipline. Special attention will be needed to ensure that the testing team has sufficient expertise, time, and resources to perform a thorough evaluation.

- Eliminate conflicts of interest in the federal testing process. ITAs should not be paid by the vendors whose systems they are testing. Several financial models are possible, and all deserve consideration. For instance, one possibility is for the EAC to collect a fee from vendors, as a condition of eligibility for the federal qualification process, to cover the costs of hiring ITAs to evaluate the system under consideration.

- Reform the federal testing process to provide more transparency and openness. All ITA reports should be publicly available. The documentation and technical data package provided to ITAs should be made available to the public or to independent technical experts so that they can independently cross-check the ITA's conclusions and exercise public oversight of the testing process. Also, the right of the public to observe elections is rendered less meaningful if those observing are unable to understand what it is that they are seeing; under the current rules, observers have no access to the documentation for the voting system they're observing, which partially limits their ability to effectively monitor the administration of the election.

- Require broader disclosure of voting system source code. The secrecy surrounding voting source code is a barrier to independent evaluation of machines and contributes to distrust. To enhance transparency, improve public oversight and hold vendors accountable, voting software should be disclosed more broadly. At a minimum, source code should be made available to independent technical experts under appropriate nondisclosure agreements. In the long run, source code should be publicly disclosed. Source code disclosure does not prevent vendors from protecting their intellectual property; vendors can continue to rely on copyright and patent law for this purpose.

  Keeping source code secret does not appreciably improve security: in the long run, the software cannot be kept secret from motivated attackers with access to a single voting machine. However, disclosing source code more broadly could enhance public confidence in elections and is likely to lead to improvements to voting system security.

- Incorporate closed feedback loops into the regulatory process. Standards should be informed by experience. At present, there is no requirement for reporting of performance data or

failures of voting equipment, no provision for analyzing this data, and no process for revising regulations in a timely fashion in response. The 2007 VVSG should incorporate a framework for collecting, investigating, and acting on data from the field and should provide a mechanism for interim updates to the standards to reflect newly discovered threats to voting systems. For instance, the FAA requires airplane operators to report all incidents (including both failures and near-failures), uses independent accident investigators to evaluate these reports, and constantly revises regulations in response to this information. Adopting a similar framework for voting systems would likely improve voting systems.

- Strengthen the evaluation of usability and accessibility. The discipline of usability has developed methods for usability testing—such as user testing with actual voters or pollworkers, as well as heuristic evaluation by usability and accessibility experts—but these methods are not currently reflected in the VVSG standards. They would represent a valuable addition to the standards. In addition, usability experts have suggested it would be helpful to move away from the current emphasis on functional requirements and towards an evaluation regime based primarily on assessing performance against some quantitative metric of usability[23]. The 2005 VVSG standards are a positive first step towards addressing human factors issues, but there is room for further improvement.

- Increase the representation of technical experts in computer security on the TGDC. The appointment of Prof. Ronald Rivest to the TGDC was warmly welcomed by security experts: Rivest is extremely qualified and very highly respected among the computer security community. However, at present, Rivest is the only member of the TGDC with substantial experience in the area of security. Appointing more TGDC members with security expertise would improve the ability of the TGDC to develop effective standards.

- Ensure that standards are grounded in the best scientific and engineering understanding. Too often, decisions have been made that do not reflect the best judgement of the relevant experts. For instance, in 2004 the premier professional organization for computing professionals surveyed their members about e-voting technology. 95% of respondents voted for a position endorsing voter-verified paper records and expressing concerns about paperless voting technologies[24]—yet two years later, this overwhelming consensus among technical experts has yet to be reflected in federal standards.

For further information, I refer readers to the ACCURATE center's "Public Comment on the 2005 Voluntary Voting System Guidelines",[25] which I have attached as an appendix to this testimony.

In the short term, adopting the recommendations of the Brennan Center report on e-voting is the most effective and practical step election officials could take to make existing voting systems as secure and reliable as possible for this November. These recommendations include:

- Conduct automatic routine audits of the voter-verified paper records;

- Perform parallel testing of voting machines;

- Ban voting machines with wireless capability;

- Use a transparent and random selection process for all audits; and,

- Adopt procedures for investigating and responding to evidence of fraud or error.

For further information, see the Brennan Center report[26].

In addition, I encourage election officials to pay special attention to their voter registration systems. In many states, voter registration processes are in a state of flux, due to the HAVA requirement that statewide registration databases be in place this year. These databases could significantly improve elections if implemented well; if implemented poorly, however, they could disenfranchise many thousands of voters. See the USACM report on voter registration databases[27].

Summary

In summary, the 2005 VVSG standards contain significant shortcomings regarding the security, reliability, and auditability of electronic voting. Members of the computer security community are available to help devise better solutions.

Notes

[1] "The Machinery of Democracy: Protecting Elections in an Electronic World", Brennan Center Task Force on Voting System Security, June 27, 2006. Since that report was written, Arizona has adopted voter-verified paper records and routine manual audits of those records statewide.

[2] "Computer loses more than 4,000 early votes in Carteret County", Associated Press, November 4, 2004.

[3] "Broward Ballot Blunder Changes Amendment Result", Local 10 News, November 4, 2004.

[4] "Broward Machines Count Backward", The Palm Beach Post, November 5, 2004.

[5] "Distrust fuels doubts on votes: Orange's Web site posted wrong totals", Orlando Sentinel, November 12, 2004.

[6] "Vote spike blamed on program snafu", Forth Worth Star-Telegram, March 9, 2006.

[7] "Analysis of Volume Testing of the AccuVote TSx/AccuView", Report of the California Secretary of State's Voting Systems Technology Assessment Advisory Board, October 11, 2005.

[8] "Analysis of an Electronic Voting System", Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin and Dan S. Wallach, May, 2004.

[9] "Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes", Science Applications International Corporation, September 2, 2003.

[10] "Direct Recording Electronic (DRE) Technical Security Assessment Report", Compuware Corporation, November 21, 2003.

[11] "Security Assessment: Summary of Findings and Recommendations", InfoSENTRY, November 21, 2003.

[12] "Trusted Agent Report: Diebold AccuVote-TS System", RABA Innovative Solution Cell, January 20, 2004.

[13] "Critical Security Issues with Diebold Optical Scan", Harri Hursti, Black Box Voting, July 4, 2005.

[14] "Critical Security Issues with Diebold TSx", Harri Hursti, Black Box Voting, May 11, 2006.

[15] "Security Analysis of the Diebold AccuBasic Interpreter", Report of the California Secretary of State's Voting Systems Technology Assessment Advisory Board, February 14, 2006.

[16] "Connecting Work on Threat Analysis to the Real World", Douglas W. Jones, June 8, 2006.

[17] For instance, the security vulnerabilities appear to violate the requirements of Section 6.4.2 and Section 6.2 of the 2002 FEC standards.

[18] "Election Officials Rely on Private Firms", San Jose Mercury News, May 30, 2004.

[19] "Election Whistle-Blower Stymied by Vendors", Washington Post, March 26, 2006.

[20] "Sort of fixed: Broader election flaws persist", Tallahassee Democrat, April 15, 2006.

[21] "Cold Shoulder for E-voting Whistleblowers", The New Standard, May 17, 2006.

[22] "New Fears of Security Risks in Electronic Voting Systems", The New York Times, May 12, 2006.

[23] "Public Comment on the 2005 Voluntary Voting System Guidelines", ACCURATE Center, submitted to the United States Election Assistance Commission, September 2005.

[24] "ACM Recommends Integrity, Security, Usability in E-voting, Cites Risks of Computer-based Systems", USACM, September 28, 2004.

[25] `http://accurate-voting.org/accurate/docs/2005_vvsg_comment.pdf`

[26] "The Machinery of Democracy: Protecting Elections in an Electronic World", Brennan Center Task Force on Voting System Security, June 27, 2006.

[27] "Statewide Databases of Registered Voters: Study Of Accuracy, Privacy, Usability, Security, and Reliability Issues", commissioned by the U.S. Public Policy Committee of the Association for Computing Machinery, February 16, 2006.