Testimony, U.S. House Subcommittee on Information Policy, Census, and National Archives

Rayburn House Office Building, Washington D.C.

Dr. Aviel D. Rubin, Professor of Computer Science
April 18, 2007

My name is Avi Rubin. I am a Professor of Computer Science and Technical Director of the Information Security Institute at Johns Hopkins University. I am also President of Independent Security Evaluators, a computer security consulting firm. I am author or co-author of several widely used books on the subject of computer and network security. My latest book, *Brave New Ballot* (Random House, 2006) is on the security of electronic voting. I received my Ph.D. in Computer Science from the University of Michigan in 1994 in the field of Computer Security. I have been specializing in research issues related to electronic voting since 1997, and I am a member of the National Committee on Voting Integrity.

In 2003, I made electronic voting my primary research focus after reviewing the source code of the direct recording electronic (DRE) voting machines used in my state of Maryland. My research team identified numerous security problems with that system, and we published a report outlining the risks of using the Diebold machines in elections. Following this academic project, I volunteered to become an election judge in Baltimore County to gain hands on experience running elections, to inform my security research. I have worked the 2004 and 2006 primary and general elections, and I am signed up to be an election judge again in 2008.

Together with several colleagues from Berkeley, the University of Iowa, Rice University, Stanford, and SRI, I approached the National Science Foundation (NSF) to establish a center for studying electronic voting. The NSF funded A Center for Correct Usable Reliable Auditable and Transparent Elections (ACCURATE) at a total of $7.5 million over five years. I am the director of the center. Our focus is on exploring the design space for voting machines so we can better understand how the next generation of these machines must be constructed. Our investigators include a psychology professor, a law professor, and eight computer scientists. The three primary goals of ACCURATE are research, outreach, and teaching. Our research focuses on developing technologies that can improve voting systems. Our outreach effort focuses on working with the elections community to help them understand technology and policy issues. For example, we participated in post-election audits in 2006. Finally, we have designed curriculum to teach our students about the important issues in electronic voting.

Our ACCURATE research consists of several thrusts. One of our projects involves performing usability testing to compare different types of equipment. We can test design prototypes against human subjects to find out whether they are usable. We also provide coordinated responses to requests, such as those from the EAC. For example, we provided detailed comments on the proposed VVSG. In addition, we are performing basic research in computer security to create technology for future generations of voting systems. For more information about the activities of ACCURATE, our 2006 annual report, which lists all of the principal investigators, as part of my written testimony is available online.[1]

[1] http://accurate-voting.org/wp-content/uploads/2007/02/AR.2007.pdf

My home state of Maryland serves as an interesting case. In 2002, Maryland began using Diebold DREs, and in 2004, the state switched to a uniform system, using Diebold DREs everywhere except in Baltimore city. In 2006, every voter in the entire state voted on a Diebold DRE. Maryland spent $106 million on its contract with Diebold. Maryland received just over $49.7 million from the federal government under HAVA. According to Maryland Board of Elections documentation, all of this will have been spent by the end of 2007.

Several studies were performed to assess the security of the Diebold DRE, including mine,[2] the SAIC report,[3] and the RABA report.[4] All of the studies found serious security problems with the Diebold machines. The media covered these studies, and public sentiment began to shift away against the use of these machines. Besides the security studies, awareness was raised that these machines cannot perform recounts, they cannot be audited, and they cannot recover from many different kinds of failures.

In 2006, the lack of resilience of the Diebold voting system to unexpected events was demonstrated by widespread failures in the September, 2006 primary. Such a complex system is inherently fragile, and some problems, that would not have resulted in serious issues in a paper-based system, disenfranchised many voters. For example, in Montgomery County, many precincts opened hours late because the smartcards needed to activate the machines for each voter were not distributed to the precincts. In my precinct, a faulty power outlet almost resulted in all of the voting machines shutting down several hours into the election. In many places, there were long lines, and in others there were missing memory cards after the close of the polls. The worst problems, perhaps, resulted from software flaws in the electronic poll books. As a poll worker, I observed many of these problems firsthand.

It is important to note that the problems with DREs are not just a Diebold problem. The problems in Sarasota County in the 13th Congressional district in Florida in 2006 demonstrate the kind of uncertainty that can accompany an election conducted on DREs. We may never know what the root cause of the problem was, perhaps a software bug or a poorly designed ballot. In either case, one in seven voters using the DREs did not have their preferences recorded, and there is no excuse for that.

Last week, the Maryland legislature voted to switch to an optical scan system with random audits due to security concerns and the myriad of problems with the DRE machines. The bill currently awaits the governor's decision. Additional motivations for this bill are the inability to audit these DREs, the inability to recover from failures and the risk of losing votes, and the inability to conduct recounts. I have been involved in the proposed legislation by reviewing drafts and making suggestions.

The Maryland legislation is designed to preserve the accessibility features of DREs. The recent generation of DREs, while problematic from a security and audit perspective, did break new ground in accessibility. It is important to note that the same accessibility features can be achieved with ballot marking devices that mark paper ballots, and accessible verification technologies are also available for paper ballots.

---

[2] http://avirubin.com/vote/analysis/
[3] http://bravenewballot.org/resources/SAIC.pdf
[4] http://www.raba.com/press/TA_Report_AccuVote.pdf

The Maryland bills in the State House and Senate are similar to the bill proposed by US Representative Rush Holt (H.R. 811) and one that is expected from US Senator Dianne Feinstein. It is not too late to fix the problems with our voting systems before any more elections are run on insecure and non-auditable platforms. It should be noted that the best technology for voting is also one of the least expensive.

DREs with which so many jurisdictions like Maryland are now saddled, cannot be properly audited. However, audits are critical components of any security sensitive system. They provide assurance that a correct result was achieved. A proper audit has the following properties:

- External to the system. For example, printing the results from a DRE and counting them does not constitute an audit.
- Publicly observable
- Reproducible
- Well defined

The goal of an audit is not necessarily to obtain the same result as in the election, but rather, to have a process where increased accuracy can be achieved with an increase in effort. A proper audit capability can also result in better failure detection and recovery.

A paperless DRE cannot be properly audited. Period. There are no records external to the system, and electronic data cannot be publicly observable. Furthermore, a DRE with a voter verified paper record (VVPR) is not as good as a paper ballot system with precinct-level op-scan counting. Here are the properties of optically scanned paper ballots that make them superior to any form of DRE voting.

- Faster voting eliminates or minimizes long lines because voters do not have to wait for machines to fill out their ballots. Scanning paper ballots takes seconds, whereas voting on a DRE takes minutes.
- Even if the equipment fails, voters can keep voting. This is not true of DREs.
- The technology is cheaper, with only one scanner and one ballot marker needed per polling place.
- Audits are do-able, and much easier to perform than with commercial VVPR systems.
- Redundant tally issues (paper vs. electronic) are simpler than in VVPR systems.
- Ballot marking systems and external verification systems make paper ballot systems as accessible as DREs, and potentially more accessible that DREs with VVPR.
- It is easier to preserve privacy than with VVPR, because most VVPR solutions store the paper records sequentially.
- It is easier to use paper that is durable.
- The operation is simpler and more transparent to voters.
- Less software is required.
- The system is simpler to administer.

Finally, I believe that NIST provided the best guidance when they suggested that a voting system is Software Independent, “if a previously undetected change or error in its software cannot cause an undetectable change or error in an election outcome.” Today’s DREs are anything but software independent, and I believe the only way to achieve software independence today is with paper ballots.