Testimony, U.S. Election Assistance Commission

Dr. Aviel D. Rubin, Professor of Computer Science
May 5, 2004

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 author or co-author of several widely used books on the subject of computer and network security, and I have chaired several of the top security research conferences. I received my Ph.D. in Computer Science from the University of Michigan in 1994 in the specialization of Computer Security. I have been researching security issues related to electronic voting since 1997. Last year, by invitation of the Department of Defense, I served on the security peer review group of the SERVE voting system for absentee voting for military personnel and overseas civilians. I also participated as a panelist in the 2000 National Science Foundation study of the feasibility of electronic voting. Last year, my research team analyzed the code used in the Diebold Accuvote TS and TSx and wrote a report citing many security flaws that we found. Our study was published in the top peer reviewed computer security conference, the IEEE Symposium on Security and Privacy. I am a member of the National Committee on Voting Ingerity, and in March, I served as an election judge in Baltimore County where Diebold Accuvote TSx machines were used.

I am here as an expert in a particular domain, namely computer security. I recognize that voting is a complicated issue with a diverse set of values, each of which is very important to the functioning of this process in a way that is reliable and trustworthy in the broadest sense. Security is a necessary component of a fair and accurate election process. However, there are other equally important components. Making sure that everyone can participate in a way that is private and independent is also key to our electoral process. Making sure that people from all walks of life, regardless of how recently they arrived in this country, can participate in the process in a language they can comprehend is also important. An accurate and secure system that limits the ability of individuals with disabilities and language minorities would fall short of meeting the goals of our democracy, as would a system that allowed everyone to participate but failed to protect the integrity and accuracy of their vote. Luckily, security and accessibility are not competing goals. While today's DREs increase accessibility, they do not provide adequate security. Appropriately designed voting systems, can provide accessibility and security. Our commitment to a fair, inclusive, secure election process requires us to demand both from our election machinery.

I come before you today to contribute my expertise garnered over years of experience as one of the leading computer security experts in my field. You will hear from experts representing the disability community and the civil rights community. They are experts in their domains. In my domain, I speak with authority. Given that we all agree that security is an important component of elections, I ask that you hear me and understand the serious nature of my critique of current DREs.

My primary concerns with today's DREs are:

- There is no way for voters to verify that their votes were recorded correctly.
- There is no way to publicly count the votes.
- In the case of a controversial election, meaningful recounts are impossible.

- The machines must be completely trusted. They must be trusted not to fail, not to have been programmed maliciously, and not to have been tampered with at any point prior to or during the election. We have techniques for building secure systems, and they are not being utilized.
- With respect to the Diebold Accuvote TS and TSx, we found gross design and programming errors, as outlined in our attached report. The current certification process resulted in these machines being approved for use and being used in elections.
- We do not know if the machines from other vendors are as bad as the Diebold ones because they have not made their systems available for analysis.

Since our study came out, three other major studies often referred to as the SAIC report, the Ohio reports, and the RABA report, all cited serious security vulnerabilities in DREs. RABA, which is closely allied with the National Security Agency, called for a "pervasive rewrite" of Diebold's code. Yet, the vendors, and many election officials, such as those in Maryland and Georgia continue to insist that the machines are perfectly secure. I cannot fathom the basis for their claims. I do not know of a single computer security expert who would testify that these machines are secure. I personally know dozens of computer security experts who would testify that they are not.

I have been disappointed that the policy community did not reach out to the computer security community when making decisions about voting technology, and when my community came to the table, they said it was too late. At first I was puzzled by the lack of attention to the security critiques of DREs. Today I am outraged. At this point the failures of current DREs have been documented in four major studies by leading computer security experts, and we have ample field experience documenting failures at the polling place. Yet computer security experts, myself included, find ourselves routinely referred to as luddites and conspiracy theorists. Failing to confer with computer security experts in decisions about voting technology was a mistake. Given the gravity of the security failings the computer security community has documented in current DRE systems it is irresponsible to move forward without addressing them.

Addressing the problems I and others have documented with DREs requires more than just fixing the machines. We must reform the process for establishing voting technology to provide transparency. Vendors are not subject to public code review. In the one instance where independent security experts had an opportunity to examine a voting system, the results proved that the current process results in machines being deployed with unacceptable lack of quality control. We cannot achieve perfectly secure systems; such things do not exist. But on the spectrum of terrible to very good, we are sitting at terrible. Not only have the vendors not implemented security safeguards that are possible, they have not even correctly implemented the ones that are easy.

If I had more time (and I would be happy to address such issues in the Q & A) I would debunk the myth of the security of the so-called triple redundancy in the Diebold machines. I would explain the limitations of logic and accuracy testing in an adversarial setting, I would explain how easy it would be for a malicious programmer to rig the election with today's DREs, and I would describe the seriousness of the security flaws that we and others have found in the Diebold machines. These are all things that I could have done and would have been happy to do, before anybody started purchasing and using these DREs. But nobody asked.

I'd like to stress one important point. Security and functionality are completely different things. Functionality is whether or not something works when it is used as planned. Functionality can be

tested, and the tests can be used to make predictions about the future behavior of a system. Security, on the other hand, has to do with how a system behaves under unanticipated circumstances with an active, dynamic adversary trying to subvert it. By definition, you cannot test a system for security the way you test for functionality. It is inappropriate and incorrect to draw conclusions about the security of a system based on its past performance. The fact that this argument is consistently put forward in defense of the security of the DREs demonstrates just how much real security expertise is needed in this process. You would not design a heart implant without feedback from cardiologists. You would not design defense systems for the physical security of this country without consulting military experts, and you should not design systems for computerized elections in this country without consulting computer security experts. I can assure you from my analysis of the Diebold machines that no such expertise was utilized.

In conclusion, my colleagues and I have presented our analysis to many different groups of computer scientists, including the National Science Foundation, the National Academy of Science, and several security conferences. We have won awards for this work, and the community at large is in strong agreement with our conclusions. I recommend that the commission heed our recommendation and seek more broad input from the computer science and the computer security communities. These people have a long history of experience with designing mission critical systems. The opinions of the experts in this matter are quite different from the picture being painted by the vendors and some state officials, all of whom have much less expertise, or no expertise whatsoever, in computer security.

Speaker Biography

Dr. Aviel D. Rubin is Professor of Computer Science and Technical Director of the Information Security Institute at Johns Hopkins University. Prior to joining Johns Hopkins Rubin was a research scientist at AT&T Labs. Rubin is author of several books including Firewalls and Internet Security, second edition (with Bill Cheswick and Steve Bellovin, Addison Wesley, 2003), White-Hat Security Arsenal (Addison Wesley, 2001), and Web Security Sourcebook (with Dan Geer and Marcus Ranum, John Wiley & Sons, 1997). He is Associate Editor of ACM Transactions on Internet Technology, Associate Editor of IEEE Security & Privacy, and an Advisory Board member of Springer's Information Security and Cryptography Book Series. Rubin serves on the board of directors of the USENIX Association and on the DARPA Information Science and Technology Study Group. He is co-author of a report showing security flaws in a widely used electronic voting system that focused a national spotlight on the issue. Rubin also co-authored an analysis of the governments planned SERVE system for Internet voting for military and overseas civilians, which led to the cancellation of that dangerous project. In January, 2004 Baltimore Magazine name Rubin a *Baltimorean of the Year* for his work in safeguarding the integrity of our election process, and he is also the recipient of the 2004 Electronic Frontiers Foundation *Pioneer Award*. Rubin has a B.S, (’89), M.S.E (’91), and Ph.D. (’94) from the University of Michigan.