Testimony of Dan S. Wallach, Associate Professor of Computer Science, Rice University

Before the Senate Committee on Rules and Administration, February 7, 2007 Hearing on Electronic Election Reform

Chairwoman Feinstein, Ranking Member Bennett, Members of the Committee:

I'm honored to have the opportunity to speak to you today about electronic voting systems, their benefits and problems, and how we might go forward to improving the technology behind our elections.

My name is Dan S. Wallach. I am an associate professor in the Department of Computer Science at Rice University. I am also the associate director of ACCURATE (A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections), which is a research center funded by a $7.5 million grant from the National Science Foundation that studies technological and policy issues with voting systems. I am presently a visiting professor at Stanford University and SRI International.

I am an expert in computer security, particularly in respect to the Internet. I became interested in voting security issues in 2001. Since then, I have published three research papers on electronic voting security issues; I have testified about voting issues to state and federal government agencies across the U.S., as well as internationally; I have assisted National Institute of Standards and Technology (NIST) and the U.S. Election Assistance Commission (EAC) in the drafting of the 2005 federal Voluntary Voting System Guidelines; and I have assisted the Carter-Baker Commission on Federal Election Reform and the Brennan Center's Voting System Security Task Force. I have also testified as an expert witness in seven electronic voting-related trials, including the ongoing *Jennings v. Buchanan* case in Florida's 13th Congressional District.

It's important to understand just how much we ask from our voting systems. We certainly want *accuracy*, both in the ability to correctly record the voter's intent and in the final tally of the votes. We also want *efficiency*, in terms of the time it takes a voter to operate the system. We need *accessibility*, to enable voters from all walks of life. We need *tamper-resistance*, to defeat attempts to corrupt the election results, whether from within or without. Problems of one sort or another will always occur, so we need *recoverability* to mitigate against such problems. We need *anonymity*, so voters may freely express their opinions without fear of bribery or coercion. Most important, we need *transparency*, such that voters, observers, and the candidates themselves can convince themselves of the correctness of the election outcome.

Achieving all of these things in voting is an impressive challenge. Mail-in ballots, for example, make sacrifices in anonymity and tamper-resistance, in return for increased accessibility and efficiency. Whenever we consider changes to voting procedures, these different features are often at odds with one another.

Nonetheless, recent paperless electronic voting systems (sometimes called "direct recording electronic" – DRE – as there is no other record of the voter's ballot) have significant problems, both in theory and in practice. An example on everybody's mind is the November 2006 general election, where the current totals have Vernon Buchanan leading Christine Jennings by 369 votes with about 18,000 "undervotes" (i.e., cast ballots with no selection in this particular race) in Sarasota County. This congressional district spans five counties; the controversy centers on Sarasota County and its use of the ES&S iVotronic paperless electronic voting system. Excluding Sarasota's absentee voters, almost 15% of the votes cast in Sarasota had no vote cast for this congressional race. If you had a result like this with punch cards or with hand-marked ballots, you would immediately suspect a flaw in the tabulating machinery and would reexamine the ballots. With paperless voting, there is virtually nothing to go back and reexamine. When the county reexamined the voting machines as part of their recount, they claimed to have found no discrepancies whatsoever. This led to a number of different hypotheses that might explain the undervote anomaly.

The **voter abstention hypothesis** simply posits that Sarasota County's voters deliberately chose to abstain from voting in the Congressional race. This seems unlikely, because no comparable undervote rate was observed in either the absentee ballots for Sarasota, or in the votes of the surrounding counties, which used different voting systems.

The **human error hypothesis** posits that the ballot style, the angle of view to the screen, the presence of two races on the same "page," or other factors in how the Congressional race was presented to voters caused some voters to "miss" the race. While the summary screen, presented immediately prior to when the voter casts a ballot, gives an opportunity for voters to recognize and correct such mistakes, some voters may not read this carefully and could likewise miss the reminder. There are several possible ways to validate this hypothesis. First, other races in Florida may have had a similar visual presentation to the page seen by voters in Sarasota County. Statistical comparisons of those county's results to Sarasota County may be able to identify whether similar populations facing a similar ballot presentation had similar undervote rates. Second, ES&S iVotronic systems could be installed in a laboratory setting and human subjects could be asked to cast ballots for fictional candidates. If the human errors occur under laboratory conditions, then they also probably occurred in the field.

The **software bug hypothesis** suggests that the ES&S iVotronic machines may have latent mistakes or errors in their design that escaped the normal testing and certification processes that are applied to all voting systems. There may be something about the ballot styles used in Sarasota County that induced the ES&S iVotronic machines to occasionally transform genuine votes to undervotes. To validate this hypothesis, we might borrow a spare voting machine, cast a large number of ballots (while videotaping everything we did), and compare the machine-reported totals to our original input. If they differed in the Congressional race, this would be a proof that the machines' software was at fault. (This process is comparable to the "logic and accuracy" testing that election officials are supposed to perform prior to every election.) Unfortunately, *such testing can never prove the absence of relevant software bugs*. The only way we could ever hope to do that

would be to inspect the source code of the voting system. Source code is the medium in which software engineers conceive and implement a computer program and is broadly considered by ES&S (and many other firms) to be a trade secret. The process of reading and analyzing the source code is labor intensive and could take weeks to perform properly. (Source code is to software engineers what blueprints are to architects. Source code is the medium in which software is created, and having it allows us to "see through the walls" and observe everything about how the system is put together.)

The **post-election corruption hypothesis** suggests that the voting machines internally recorded votes correctly, but that the vote records were somehow corrupted, perhaps by poll workers or election administrators, before they were tallied and presented as official results. To test this hypothesis, we must require that the original voting machines were properly sequestered and protected (i.e., their chain of custody was properly maintained at all times). Then, we could directly download voting records from each machine and tabulate them ourselves. If we found any discrepancies, that could be indicative of corruption. (This is approximately what Sarasota County did as part of their recount process. They claim to have found no anomalies.)

The **malicious software hypothesis** considers that the software or firmware inside the voting machines might have been illegitimately modified in such a way as to introduce bias into the machine's cast vote records. Testing this hypothesis would require physically disassembling the voting machine to access its internal memory chips and extract their contents for suitable forensic analysis. This process is labor intensive and would take weeks to perform properly. Even then, it's technically feasible for malicious software to overwrite itself, i.e., to erase its tracks.

Unfortunately, we do not yet have enough information to determine which of these hypotheses (or what combination of these hypotheses) would explain the anomaly. Certainly, the ballot layout has come under justifiable criticism from human factors experts, but we don't know if it's enough to explain the high undervote rate. Likewise, ES&S has publicly described relevant software bugs in its iVotronic system[1]. Perhaps a similar issue occurred in Florida.

A commonly suggested solution to these problems is the use of a *voter-verifiable paper audit trail* (VVPAT). This could take the form of a printer, attached to the voting machine, which produces a list of the candidates selected by the voter. The voter reads it and verifies its accuracy. The printout then goes into the ballot box. Broadly speaking, the paper is then considered to be the ballot, and would take precedence over any electronic tallies. Likewise, hand-marked paper ballots / optical-scan ballots have this same property: the voter can read and verify a tangible record of their vote, rather then the ephemeral contents of a computer screen. More generally, a recent NIST report[2]

---

[1] Letter from Timothy J. Hallett, on behalf of ES&S, to Keith Long, a project manager in North Carolina's State Board of Election, March 14, 2006, stating that under certain circumstances, the write-in vote option would not appear on the screen. ES&S claimed this occurred "two to three percent of the time."

[2] "Requiring Software Independence in VVSG 2007: STS Recommendations for the TGDC," November 2006. `http://vote.nist.gov/DraftWhitePaperOnSIinVVSG2007-20061120.pdf`

referred to this property as *software independence*, meaning that an election can be tallied without requiring that any official software be working properly. If the official software were malfunctioning, others could build their own software, or perform counts by hand.

Vendor Trade Secrecy vs. Election Transparency

A significant problem in the Florida case, as well as in any other case where the paperless voting machines yield questionable results, is the inability for the aggrieved candidates, their representatives, or members of the general public to learn anything about what might have gone on inside those voting machines. Voting system vendors have vigorously resisted attempts to allow independent experts to examine the inner workings of their voting systems. Whenever such experts have performed analyses, they have found significant problems. For example, in a paper I co-authored with Prof. Aviel Rubin (Johns Hopkins), Adam Stubblefield, and Tadayoshi Kohno[3], we found significant security flaws in Diebold's AccuVote-TS voting system, including a design flaw that would allow a voter to cast multiple votes. Subsequent work by a group of Princeton researchers[4] found that the Diebold machines use a physical lock that can be opened with common hotel minibar keys. They demonstrated that the Diebold machines were vulnerable to a *voting system virus* which could spread from machine to machine by piggybacking on the memory cards which are used to set up and close out elections[5].

Diebold and every other major voting system vendor maintain that an open discussion of flaws in their voting systems would somehow make it easier for somebody to exploit those flaws. This notion is sometimes referred to as "security through obscurity" and has been widely discredited for centuries, starting with locksmiths who realized the importance of widely discussing good lock design, to best overcome the rogues of the day. The same issue applies to voting systems. Those who might wish to corrupt an election will have no qualms about stealing a machine and reverse-engineering it. Whatever modest gain is made in security is immediately offset by a huge loss of transparency[6].

"Fear not," we are told, because these voting machines are *certified*. For the voting machines used in the recent November 2006 general election, that generally meant that one or more independent testing authorities (ITAs), as blessed by the National Association of State Election Directors (NASED), conducted an examination relative to

---

[3] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach, Analysis of an Electronic Voting System, *2004 IEEE Symposium on Security and Privacy* (Oakland, California), May 2004. `http://avirubin.com/vote/analysis/`

[4] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, "Security Analysis of the Diebold AccuVote-TS Voting Machine," September 2006. `http://itpolicy.princeton.edu/voting/`

[5] Most computer viruses, today, spread via computer networks. Before networks were common, computer viruses were still a real problem and would spread via infected floppy disks. Diebold's voting system is vulnerable to this style of attack.

[6] The security through obscurity issue, as it pertains to voting systems, is discussed in detail in Jason H. Tokoro, Sarala V. Nagala, and Jack I. Lerner's "Disclosure of Information Regarding Electronic Voting Systems," a letter to Minnesota's Secretary of State, Mark Ritchie, December 2006. `http://www.law.berkeley.edu/clinics/samuelson/LtrtoMNSoSRichie.pdf`

the 2002 Federal Election Commission "voluntary" voting system standards (VSS), which are incorporated into many states' statutory requirements.[7] In *Conroy v. Dennis*, a lawsuit filed in Colorado against Colorado's then-Secretary of State, Prof. Doug Jones (University of Iowa) and I were engaged as expert witnesses on behalf of the plaintiffs to carefully study the certification documents[8,9] which are, themselves, considered to be trade secrets owned by the vendors and sometimes provided to the states. We found that the certification process was insufficient to address many security and reliability concerns.

Starting from a young age, children are taught in science and mathematics classes to "show their work." A fundamental tenet of science is that a research report must present enough information for an independent observer to replicate the same result. This level of rigor is equally critical for the analysis and certification of voting systems. None of the reports read by myself or Dr. Jones showed their work in any regards toward computer security issues. For some critical areas, such as telecommunications support, the voting systems were not subject to any testing at all. Because telecommunicated results are considered "unofficial," no scrutiny was considered necessary for that aspect of the system. In fact, once you have a modem connected to a computer in the election administrator's office, for whatever reason, you have an avenue through which the system might be attacked.

As an example, while Wyle's analysis of ES&S was quite superficial, it did inadvertently point out significant problems in ES&S's software engineering process. Wyle's "Change Release Report of the ES&S iVotronic (Firmware 8.0.0.0)" (February 2004), details a back-and-forth exchange between Wyle and ES&S concerning a variety of different iVotronic software releases:

> 8.0.0.0ZM: received at an unspecified date
> 8.0.0.0ZZD: received July 16, 2003
> 8.0.0.0ZZH: received July 25, 2003
> 8.0.0.0ZZI: received July 29, 2003
> 8.0.0.0ZZJ: received August 15, 2003
> 8.0.0.0ZZL: received September 10, 2003
> 8.0.0.0ZZM: received September 29, 2003

It required five round-trips between ES&S and Wyle before Wyle was willing to consider the ES&S software (version 'ZZJ) to be in compliance with the 2002 FEC guidelines. The protective order in *Conroy v. Dennis* precludes me from directly quoting the Wyle report, but similar exasperation with ES&S's inability to address its poor software

---

[7] This will be shifting to the newer 2005 voluntary voting system guidelines (VVSG), under the aegis of the Election Assistance Commission, for 2007 and thereafter.

[8] Dan S. Wallach, "Expert Report in *Conroy v. Dennis*" (portions redacted), September 2006. `http://accurate-voting.org/wp-content/uploads/2006/09/dwallach-redacted-new.pdf`

[9] Douglas W. Jones, "Expert Report in *Conroy v. Dennis*" (portions redacted; with bibliography), September 2006. `http://www.cs.uiowa.edu/~jones/voting/conroy_v_dennis_jones.pdf`

engineering process is evident from the public report of Dr. James Sneeringer, a voting system examiner for the Texas Secretary of State[10]:

> ES&S presented us with two sets of software change logs, one with their initial submission and another when they presented additional equipment to be examined. The changes listed appear to be completely different, even though the logs were for the same product and in some cases covered the same version range and the same data range. This examiner attempted to match the changes listed in the two reports, on the assumption that they were the same changes but were reported in a different order and worded slightly differently, but found almost no duplication between the reports. ES&S told us that the newer reports are the accurate ones, but they offered no satisfactory explanation of where the other reports came from. At the exam, they submitted a third set of reports that were consistent with the second set, the only differences being some entries for additional changes made since the second set of reports.
> …
> **Recommendation**: Certification should be denied unless there is a satisfactory explanation. A development process that produces reports with contradictory information is not acceptable, and the integrity of the examination process relies on examiners receiving correct information from vendors.

The rapid back-and-forth between ES&S and Wyle is directly indicative of an ad hoc software development and testing process within ES&S. The Texas examiner's observations indicate that this was not an isolated incident. A poor software engineering process is virtually guaranteed to yield low quality code, leading directly to a higher likelihood of software failures and security vulnerabilities. I agree with the Texas examiner's conclusion that this raises significant concerns about the vendor's ability to deliver systems of the necessary quality to run elections, yet this is the very same system that was used in Sarasota County, Florida, yielding about 18,000 undervotes in Sarasota County.

Recommendations

I generally support legislation, such as Rep. Rush Holt's bill, that would require any electronic voting system to have a voter-verifiable paper trail and for that paper trail to be audited before the election results are certified. More deeply, we need to reconsider whether trade secrets, of any form, are appropriate within the electronic voting systems industry. Trade secrets cut directly to the heart of election transparency, they are counterproductive for security, and they are unnecessary for the protection of companies' intellectual property (which can be adequately protected with copyrights, trademarks, and/or patents). We also need standards with stringent requirements on how machines are designed, engineered, and tested, and more transparency into the testing process so

[10] James Sneeringer, Ph.D, "Voting System Examination: Election Systems & Software (ES&S)," June 2004. http://www.sos.state.tx.us/elections/laws/may2004.shtml

we may satisfy ourselves that voting system evaluation is sufficiently rigorous. Of course, these standards must pay attention to security and reliability, but they must also pay more attention to usability for voters and for poll workers. Engineering and testing voting systems is an impressive technical challenge, and it will require a broad effort to adequately address our country's needs. Thank you.