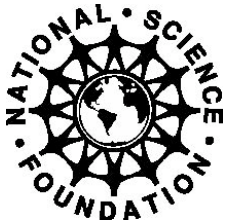
ACCURATE: A Center for Correct Usable Reliable Auditable and Transparent Elections

2007 Annual Report



Funded by the National Science Foundation under the CyberTrust program. Grant Number CNS0524252

Overview

2007 was a very productive year. ACCURATE co-PIs produced many new research results in all of our core areas, including system level issues, the role of cryptography, design for verification, relating policy to technology, and usability and accessibility. This report provides the details on these developments. As this year lies in between two national election years, the thrust of our outreach activities lay in post-election analysis of the 2006 election and preparation for the 2008 Presidential election. A particular highlight of this year was the California Top to Bottom review of their voting systems, which was called for by the Secretary of State and ACCURATE advisory board member, Debra Bowen, and led in part by ACCURATE center co-PI David Wagner. That comprehensive study, which included other ACCURATE members as well and which is described later in this report, resulted in several decertifications of voting systems in California and prompted other states to re-examine their voting systems. The impact of the California top to bottom review was tremendous and is an example of ways in which ACCURATE members are influencing real elections.

This year, ACCURATE co-PIs and their students have tested voting systems in several states and multiple countries, helped design voting technology legislation, and testified before committees of local, state, and the federal governments. Center activities have once again been featured in the New York Times, the Washington Post, Newsweek, Time Magazine, and on NPR and CNN, as well as many other media outlets.

Co-PI David Wagner co-chaired the Electronic Voting Technology 2007 workshop, together with Ray Martinez (former Commissioner of the U.S. Election Assistance Commission). EVT is an annual workshop co-sponsored by ACCURATE and by USENIX. The EVT 2007 workshop was phenomenomally successful. We received 44 submissions (a 158% increase compared to EVT 2006) and accepted 16 papers. This indicates that EVT is healthy and reflects a growing interest among the research community in electronic voting technology.

One of the goals of the EVT workshop was to help grow a community of researchers working in this field. This appears to have been successful: 5 of the 16 published papers at EVT 2007 were authored by ACCURATE researchers, and the other 11 papers came from other organizations. Also EVT 2007 was successful at attracting scholars from multiple disciplines: 2 published papers came from legal scholars, and we noticed many attendees from disciplines other than computer science. Plans for EVT 2008 are underway; it will be co-chaired by Tadoyoshi Kohno (University of Washington) and ACCURATE Co-PI David Dill.

Education is a core component of the ACCURATE center. To date, numerous college courses covering electronic voting were taught or co-taught by our co-PIs, and several new ones are planned. The courses have engaged students in the democratic process, taught them about the hot issues, and provided them the opportunity to solve some problems related to elections and technology. ACCURATE has provided funding for 21 graduate students, 17 undergraduates, and one post-doc.

The ACCURATE center engages in an unusually large amount of outreach for a research center due to the important applicability of our work to actual elections. The outreach activities can be broadly categorized into three areas, namely, working with election officials and participating in elections; post-election auditing and analysis; and raising awareness of security and other issues via hearing testimony and working with the press. Our far reaching outlook has had a direct impact on many elections, and as can be seen from our detailed activities section below, many election officials and jurisdictions rely on ACCURATE for support.

Finally, our center advisory board welcomed 2 new members, Professor Ed Felten from Princeton and David Klein from the Ohio Secretary of State office. A complete list of our external advisory board can be found in Appendix B of this report.

As the 2008 election approaches, ACCURATE expects to make great contributions in every aspect of the elections including election observation, working at the polls, incident recording, statistics gathering, voting system analysis, and post election evaluation.

Detailed Activities

This section provides details on the 2007 center activities. ACCURATE has been very successful in pushing the state of the art in technology, usability, and policy research. Furthermore, given the practical importance of electronic voting, there has been an unusually large amount of outreach and contribution to the elections community. Finally, the problem of electronic voting provides a tremendous opportunity for educating students and involving students in research projects. A list of our center publications appears in Appendix C.

Research

ACCURATE's research goals are divided into 5 broad categories: System-Level Issues, The Role of Cryptography, Design for Verification, Relating Policy to Technology, and Usability and Accessibility. This section provides an overview of the research in these areas.

System-Level Issues

This section describes the ACCURATE projects relating to system-level issues.

- Dill, his students, and their collaborator Eric Lazarus (Brennan Center for Justice, NYU) are using their AttackDog threat modeling system in a study to compare the severity of threats of various classes of election fraud. This analysis includes over 9,000 attacks, including attacks on computer technology, vote-by-mail, vote suppression, and voter impersonation. When completed, they expect this study to provide an objective basis for further debate about how to prioritize election security measures.

- With the office of the Supervisor of Elections, Leon County, Florida, AttackDog

and the methodology Dill and his collaborators have developed are being used to investigate security flaws and analyze countermeasures to election fraud. There office is doing detailed proofreading and analysis of our threat models, helping them find errors and omissions in our attack trees. These threat models will be used to recommend changes in legislation, regulations and changes in practice in Leon County itself.

- Optical mark-sense ballot counting and direct-recording electronic voting machines both offer significant opportunities for post-election auditing, but these audits are not equivalent. In auditing an election conducted on a DRE voting machine with a paper trail, the audit does not cover the effectiveness of the user interface in accurately capturing the voter's intent. In contrast, a post election audit of mark-sense ballots can discover all of the different ways voters reacted to the ballot, including numerous misunderstandings of the ballot marking instructions. Douglas Jones and two of his students, Robert Hansen and Mark Slayton, have begun an investigation of the consequences of this difference, both from the point of view of the interpretation of post-election audits and from the point of view of how the event-logging mechanisms of direct-recording electronic voting machines might be modified to monitor vote-capture problems without endangering voter privacy.

- Peter Neumann has published a book chapter, Reflections on System Trustworthiness, Advances in Computers, Vol. 70, 2007, pp. 269-310. This chapter examines approaches that might achieve dramatic improvements in the ability to develop, operate, and use trustworthy systems. It includes a section on risks in electronic voting systems, and illustrates the applicability of various principles of system architecture and system development to election systems.

- Dan Wallach, Rice graduate student Dan Sandler, and Rice undergraduate student Kyle Derr have designed and implemented a system called “Auditorium” that forms the base of a voting system prototype called “VoteBox.” Auditorium is a networked logging and auditing system built from timeline entanglement and broadcast messages. Auditorium allows anybody to audit the events, in the order that they occurred, with strong cryptographic guarantees to protect against tampering with the timeline. This was the subject of a 2007 EVT paper. Further research on secure logging is currently in submission at another security conference, and ongoing research is considering how such log verification might scale to an entire election in real time.

- Arel Cordero and David Wagner are studying methods for building trustworthy audit logs in electronic voting systems. In particular, their goal is to design a mechanism that records the entire user interaction between the voter and the voting machine and allows auditors to replay a “movie” of that interaction after the election. The research challenges are to ensure that this audit log does not compromise ballot secrecy and that it is trustworthy. This is work in progress.

The Role of Cryptography

One of the areas of research that is critical to ACCURATE is in the area of Cryptography. The following are cryptography-related projects within ACCURATE:

- Automatic formal verification of block cipher implementations. Dill and Boneh have developed a system for fully automatically proving that the Java object code implementations of block ciphers are functionally equivalent to their specifications. They have successfully verified the compiled Java code for the Bouncy Castle provider for the Java Cryptography Extension (JCE) including three implementations 128-bit AES, DES, RC6, Blowfish. They've also verified that SHA-1 and MD5 work for all 32-bit and 512-bit messages. Dill and Boneh have also verified the Sun provider implementations for AES, DES, and Blowfish. In each of these cases, they proved the implementation equivalent to a logical specification if the appropriate standard. They also proved that the Bouncy Castle and Sun implementations of RC2 are equivalent. This system is implemented on top of the ACL2 theorem-prover and STP, a decision procedure for bit-vectors.

- Dill and Boneh have developed a framework for formally verifying security and reliability properties, simultaneously. This is important since focusing on those properties individually may fail to notice conflicts between them. For example, lost cryptographic keys can lead to data loss (or, equivalently, the inability to decrypt data). Dill and Boneh became concerned about this issue when considering the consequences of cryptographic key loss during an election, which could render voting machines unusable and data inaccessible. They are using the XSB logic programming system to model systems and attackers, and to prove the desired properties. They are applying these ideas initially to parts of Microsoft Vista's "BitLocker" drive encryption system, which provides several alternative ways of backing up encryption keys.

- The Rice VoteBox system uses a variety of cryptographic primitives to ensure that data on the polling-place network is secure from eavesdroppers. Working in collaboration with Brent Waters, we are applying homomorphic encryption techniques, non-interactive zero-knowledge proofs, and other related techniques to VoteBox. This is work in progress.

Design for Verification

One of the novel concepts in our ACCURATE grant proposal was the idea that systems can be designed for verification. That is, that verification is one of the key properties of a voting system, and it should be designed for, just as performance and scalability are often designed for in computer systems. This section describes our research into verifiable voting systems.

- Dan Wallach, Dan Boneh, and David Dill wrote a paper on several options for making vote-by-mail more secure. Part of the preparation for this work involved meeting with the staff of the San Mateo County elections office to understand

their processing of absentee ballots.

- The Auditorium network system was designed to be verified by each of its network participants (i.e., networked voting machines in a local precinct). In future work, we are examining ways to extend auditable information out of the precinct to the Internet (one way only!) in order to allow real-time auditing of voting as it happens, all without compromising voter anonymity and privacy. This is joint work between the Rice group and Brent Waters at SRI.

- Naveen Sastry completed his Ph.D. dissertation, titled "Verifying Security Properties in Electronic Voting Machines." The dissertation introduces three techniques for making it easy to verify that voting machines satisfy certain security properties. The thesis starts at the level of public policy, identifying high-level goals that we expect voting machines to meet, and shows how to translate them into specific technical requirements that can be evaluated.

  Naveen's dissertation makes several technical contributions. First, Naveen shows how to prove that a voting machine preserves ballot secrecy and treats all voters equally by demonstrating that the machine retains no memory of past interactions with previous voters. His idea is to simply reset the voting machine after each voter is finished with it, and verify that there is no other way for the voting machine to gain any information about past voting interactions from non-volatile storage. Second, Naveen shows how to architect a voting machine so that the "summary screen" will be trustworthy. In DRE voting systems, before the voter casts her ballot, she is shown a screen summarizing her selections and asked to confirm those selections. Naveen shows how voting software can be constructed so software reviewers can verify that the vote cast will accurately reflect what was shown to the voter on the summary screen. This work involves using hardware isolation and appropriately chosen software architectures. Third, Naveen shows how to verify that the electronic vote record will be interpreted by the back-end tallying software, when the votes are counted, in the same way that it was interpreted when displaying the summary screen to the voter.

  His work is likely to have applications outside of e-voting. Reset-based privacy is applicable to a broad range of kiosk devices. Also, he devised a novel a solution to a specific problem in verification of software correctness: Given two functions f(), g() implemented in Java, prove that g() is the inverse of f() on the inputs where it is applied. He implemented his solution and demonstrated that it is practically useful.

- We completed a security review of Ka-Ping Yee's Pvote prototype voting software. We recruited leading security and voting researchers (including Dan Wallach, Dan Sandler, Matt Bishop, Yoshi Kohno, Mark Miller, and Ian Goldberg) to perform an independent security evaluation of our software. The reviewers spent a total of about 90 hours analyzing the Pvote software. The review exercise was unusual in that it was an adversarial code review: we

informed the reviewers that they were not to trust the author of the program, because we intended specifically to address the insider threat. The reviewers did not find any bugs or flaws in Pvote, and they concluded that Pvote had probably been more thoroughly scrutinized than the corresponding part of any commercially available system.

The review also revealed an important surprise. As part of the exercise, Ka-Ping Yee and David Wagner deliberately introduced three bugs into the software to see if the reviewers would find them. The reviewers found some but not all of these bugs, even after being told of their existence and given a narrow range of 100 lines of code where the bugs were hidden. The conclusion we drew is that it is extremely difficult to find intentionally hidden bugs and backdoors, even with intense scrutiny and a limited code size. The security review also taught us several lessons about how such reviews should be conducted.
Ka-Ping Yee completed his Ph.D. dissertation, titled "Building Reliable Voting Machine Software." His Ph.D. includes his research on pre-rendering, Pvote, accessibility, and the Pvote security review.

- Sujata Garera, Ryan Gardner, and Avi Rubin examined the possibility of a mechanism by which a poll worker, on election day, could validate that the software in a voting machine is the software that was produced by the vendor, without requiring a computational device. Our contribution highlights the difficulties in achieving voting software integrity and demonstrates that it is extremely unlikely that current software attestation techniques can provide security for electronic voting. To detect violation in integrity of voting software, we relied on Pioneer, a software based tool for verifying the integrity of code execution. Pioneer attempts to provide a mechanism for validating that correct code is running based on some of the performance characteristics of the computer. In particular, it relies on the fact that certain operations would require a noticeable increase in computation time if code were modified. We extended the Pioneer primitive so that the time difference between a run with legitimate software and one with modified software is easily discernible by a poll worker. We implemented a framework for measuring the integrity of the Diebold voting software at boot time using Pioneer, on an Intel Core 2 Duo machine. We further implemented an attack on our system, to demonstrate its human verifiability. Our results however surprised us, and demonstrate a considerably low percentage attack overhead compared to that observed by the Pioneer authors. We believe that the most probable explanation for this concerns CPU architecture. We hypothesize that as instruction level parallelization technology advances, the already minute overhead of the attack on our current implementation will diminish further, demonstrating that the current state of art in software based attestation is not robust enough to be deployed on newer architectures for providing human verifiable attestations of voting software. The paper was published in EVT 2007.

- Sujata Garera and Avi Rubin designed a framework for auditing DREs. The

framework does not impose many hardware and software changes in the current DRE system. Rather than addressing privacy issues that arise in voting systems, we focus on a design can be easily deployed and which is extensible. The basic intuition behind our method is to capture the input into the software and accordingly determine the correct output. In the voting setting, the input is the vote cast by a user and the corresponding output involves incrementing the respective candidate counter. If an execution flaw is detected during input capture then an alarm is raised. Through such an independent audit, it is possible to later check (after the election is over) if the voting software produced the correct outcome or not. This assumes that we trust the independent audit mechanism. Our audit mechanism, determines the input entered by the voter by screen capture and image comparison techniques. To ensure that flaws (both intentional and otherwise) in the voting machine are not propagated to the audit, it is important that the audit mechanism itself be separated from the voting software. We achieve this isolation through system virtualization. We find that with the virtual introspection based architecture, we can maintain an accurate audit. Our image comparison techniques produce a negligible overhead on input capture. We find that our architecture is robust in the condition that the ballot definition file has not changed. The paper was published at the ACM CCS conference.

Relating Policy to Technology

This section describes the ACCURATE research related to the nexus of policy and technology.

- David Dill and Dan Wallach wrote a white paper titled "Stones Unturned: Gaps in the Investigation of Sarasota's Disputed Congressional Election." on the investigation of the unusually large undervote in the 2006 U.S. Congressional District 13 race in Sarasota Florida, which may have affected the outcome of the election. This paper was widely circulated and influenced and continues to influence the still-ongoing investigation by Congress. It is available on the web at: http://www.cs.rice.edu/~dwallach/pub/sarasota07.pdf

- Douglas Jones's work on the white paper "From Power Outages to Paper Trails", distributed at the IFES Global Electoral Organization conference, incorporates large amounts of the material originally presented at the first ACCURATE site visit; the IFES GEO audience is composed largely of election administrators from around the world.

- We are well into a multi-year analysis of contractual relationships between voting system vendors and election jurisdictions. These contractual arrangements are influential in that they are the primary organizational artifacts of the U.S. voting system market. The first step in this project was to collect a large number of such agreements and perform a qualitative analysis of their terms. As part of his PhD thesis, Joseph Lorenzo Hall examined a set of 55 such contracts for terms that could affect transparency in terms of inhibiting access to information about the

voting systems, oversight activities in which election officials might wish to engage and efforts to promote accountability. Hall's paper was published in the 2007 USENIX/ACCURATE Electronic Voting Technology Workshop.

- This project will continue with a more comprehensive analysis of voting system contracts from the perspective of transaction cost economics (TCE). This framework will allow us to tie together many of the legal and institutional forces that have influenced—and continue to influence—the course of voting system technology's development, including election law, testing and certification, and intellectual property law. Our study will not only lead to a better understanding of how variables such state laws, size of jurisdiction, and experience with electronic voting systems affect the terms of these contracts, but will also allow us to develop specific recommendations for contract language that jurisdictions may use.

- Members of the ACCURATE policy group participated in the California Top-To-Bottom Review of voting systems and the Ohio Evaluation and Validation of Election-Related Equipment, Standards and Testing (EVEREST) review of voting systems. These two reviews constitute the most comprehensive technical reviews of the voting systems manufactured by the four dominant voting system vendors (Election Systems and Software, Inc., Premier Election Solutions, Inc. (formerly Diebold Election Systems, Inc.), Hart InterCivic, Inc. and Sequoia Voting Systems, Inc.). In these reviews, the role of ACCURATE policy group members encompassed technical document review in terms of adequacy of past testing performed, document sufficiency, usability and completeness as well as policy, procedure and legal analysis.

- In conjunction with the Brennan Center for Justice at the NYU School of Law, we have completed a review of models for conducting post-election audits and how States are approaching this important part of the elections cycle. We convened a blue-ribbon panel of experts for this analysis for meetings over a one-year period and then published a whitepaper.

- Joseph Lorenzo Hall was invited by the California Secretary of State to present testimony in front of her Post Election Audit Standards Working Group. Hall's testimony covered post-election audit models as well as specific issues that make post-election audits difficult in the California environment. The output from that working group has since been incorporated into standards for post-election audits for the 2008 election season in California.

- We have also been working on extending ACCURATE's influence in voting system regulation at the federal level. The next major watershed in the evolution of voting system regulation is the development of the U.S. Election Assistance Commission's Voluntary Voting System Guidelines II (VVSG II). The VVSG II is a complete overhaul of national voting system certification guidelines and has been released in draft form for public comment. ACCURATE's comments in

2005 were highly critical of the Guidelines released that year and appear to have influenced the new version. ACCURATE will be submitting extensive comments supporting the thrust of the new standard, especially the concepts of software independence, vulnerability testing and the new usability and accessibility standards. Our comments will also address the level of institutional support needed to make the standard effective as well as the long-term prospect for expert input into the standard.

Usability and Accessibility

This section describes the ACCURATE research related to usability and accessibility.

- We continued the previous year's project on prerendered-interface architectures for high-assurance voting machine software, extending our design and development work to support accessibility. The specific aim of this project was to create the smallest, simplest, and most easily verifiable vote-entry software possible. The result, which we call Pvote, consists of just 460 lines of Python. Despite its small size, it offers a synchronized audio and video interface to the voter, provides support for accessible input devices, and handles a wide range of ballot features and designs.

  This works demonstrates how to use pre-rendering to build voting machine software that is usable, accessible, and well suited for verification. Complexity is one of the primary barriers to formal verification as well as to informal code review. The goal behind pre-rendering is to dramatically reduce the complexity of voting machine software and therefore make it more amenable to verification. In past work, we have demonstrated that pre-rendering can be very effective at this, and we built a research prototype voting machine that uses the pre-rendering approach. However, that prior work was not accessible to blind voters, voters with vision impairments, and others.

  Pvote illustrates how to extend pre-rendering to support accessibility. Pvote provides support for blind voters, voters with vision impairments, voters with motor impairments, voters who prefer to vote in other languages, and other categories of voters. This work demonstrates that we can greatly reduce the complexity (and thereby improve the verifiability) of voting machine software while providing the same level of accessibility provided by current commercial systems. This work was published at EVT 2007.

- We had several findings from the VoteBox software project in our usability studies:

  - Our initial findings are that the voters in our studies have a strong subjective preference for VoteBox, but this is not accompanied with any benefits in objective performance in terms of faster voting or fewer errors. This is an important disconnect; because voters like these systems, they may believe

they are faster and more accurate, and they may resist change. Both may contribute to additional resistance to reforms in DRE platforms.

- The second major finding using VoteBox was reported in Sarah Everett's dissertation. In that work, we had the final "review screen" (a common feature of DREs) present something to the voter, which disagreed with their selections. We either added or removed entire races, or changed votes from one selection to another. Approximately two-thirds of our participants did not notice this change. Factors most closely related to noticing were unsurprising: voters who spent more time on the review screen were more likely to notice, and voters who were instructed on what choices to make also were more likely to notice. Interestingly, the number of changes made to the review screen was not a factor. We will soon be conducting a follow-up experiment where we attempt to manipulate the aggressiveness with which the DRE prompts voters to check the review screen to see if this makes a difference.

- The third VoteBox-based finding was the effect of altering the navigation model. Most commercial DREs and the original version of VoteBox force voters to navigate through every single race on the ballot, even if they choose to abstain, they still see every race. Wallach's team constructed a version of VoteBox which used a different navigation model, one in which voters could navigate to any race they wanted in any order they wanted. This had a substantial effect on voter performance: voters made substantially more errors with this version, in particular, they made many more undervotes. In fact, they not only made more erroneous undervotes, but those voters who made selections on their own also chose to vote in substantially fewer races overall.

- Finally, we have recently developed a version of VoteBox in Chinese, which we will be using to collect data soon. Shortly thereafter, we intend to develop a Spanish version as well.

- We have done research examining the rate and accuracy with which thermally-printed rolls of VVPATs can be counted. Our initial study indicated that counting these records is both slow and inaccurate, but it is particularly inaccurate when races are lopsided in the outcome and the rate of rejected VVPATs is high. This is a preliminary result and we will be conducting a follow-up study in the coming year to better understand this effect as well as to compare VVPAT counting with alternative auditing procedures such as hand-counting optical-scan ballots and team-based counting procedures.

Education

This project has provided outstanding opportunities for students. In addition to courses on electronic voting and broader courses that covered voting, ACCURATE members participated in educational activities such as VoComp 2007, a university voting competition where Doug Jones served as a judge. This section provides an overview of

courses that were developed and taught and students who have received training through the center's activities.

Courses

ACCURATE researchers incorporated electronic voting topics into their courses. The following courses and course projects took place under our NSF funding.

- Douglas Jones taught 22C:169, Computer Security, in the Spring of 2007, incorporating several examples from the election domain.

- In the Spring '07 and Fall '07, Avi Rubin taught CS 443, Security and Privacy in Computing, and the course material and lectures covered electronic voting security in detail.

Students

The following students have been funded under the ACCURATE center grant:

- Johns Hopkins University:
    - Graduate students: Sujata Doshi, Ryan Gardner, Josh Mason

- University of Iowa:
    - Graduate students: Robert Hansen, Andrea Mascher
    - Undergraduate students: Tom Bowersox, Patrick Holley, Tristan Thiede, Mark Slayton

- University of California at Berkeley:
    - Graduate students: Arel Cordero, Naveen Sastry, Ka-Ping Yee, David Molnar, Chris Karlof, Joseph Lorenzo Hall
    - Undergraduate students: Chris Crutchfield, David Turner, Drew Lewis
    - Clinical Interns: Stephen Dang, Galen Hancock, Cecilia (Peggy) Walsh, Erica Brand, Jason Tokoro, Sarala Nagala
    - Post Doc/Fellows: Aaron Burstein

- Stanford University:
    - Graduate students: Eric Smith, Sean Ting
    - Undergraduate students: Tim King

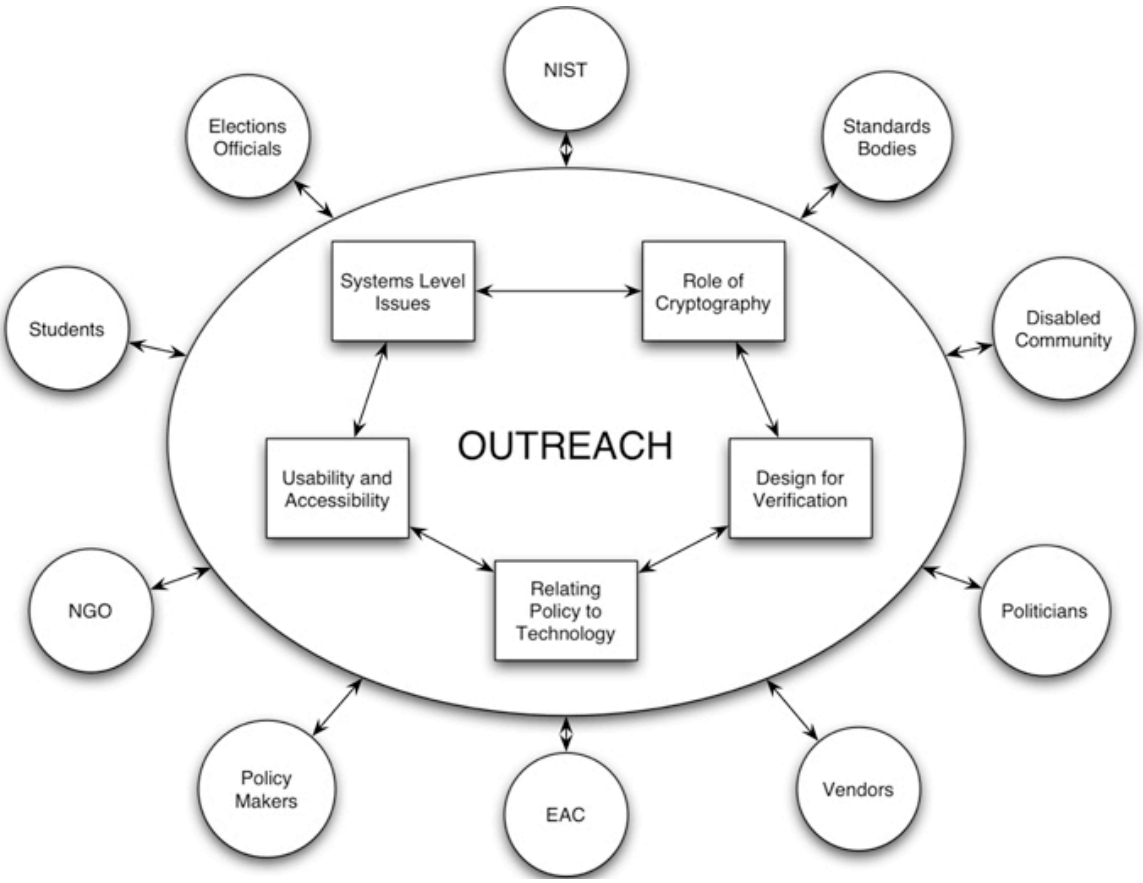
- Rice University:
    - Graduate students: Dan Sandler, Bryan Smith, Sarah Everett, Kristen Greene, Bryan Campbell
    - Undergraduate students: Liz Guillen, Amy Lin, Stephen Goggin, Diego Caballero, Kyle Derr (also summer intern at SRI), Corey Shaw, Ted Torous, Adam Purtee, Emily Fortuna

- Other Institutions:
    - John Bethencourt, CMU

- Tadayoshi Kohno, UCSD
- Ryan Moriarty, UCLA

Outreach

When ACCURATE was first proposed, it was clear that the outreach component of the center was going to be central to our activities. This was displayed in our initial site visit presentation with the following graphic:



The picture illustrates that the primary research areas feed into our outreach program, which involves many different organizations such as the EAC, politicians, NIST, the disabled community, and the other parties who are features in the diagram. This section will describe ACCURATE's outreach activities in 2007. The activities fall into three broad categories:

1. working with election officials and participating in elections
2. post-election auditing and analysis
3. raising awareness of security and other issues via hearing testimony and working with the press

The remaining subsections provide details of these outreach activities of ACCURATE.

Working with Election Officials and Participating in Elections

One of the strengths of ACCURATE is the close tie that we've developed with members of the elections community. Our board of advisors, for example, includes the co-chair of the New York State Board of Elections, the Secretary of State of California, the Assistant Secretary of State of New Hampshire, the Chief Deputy Clerk/Recorder for Yolo County, California, and the former chairman of the EAC. In addition to these resources with whom we speak frequently, center members have worked closely with other elections officials. Here are some of the specific activities that took place in 2007:

- David Wagner continued his service on the U.S. Election Assistance Commission's Technical Guidelines Development Committee. The TGDC is the committee charged with helping to draft the next federal voting standards. The TGDC completed their draft of the voting standards this summer and transmitted them to the EAC for public comment and revision. Wagner serves on the TGDC as the representative of the American National Standards Institute (ANSI).

- David Wagner joined the Overseas Vote Foundation as Special Advisor to the Board, Security and Privacy. The Overseas Vote Foundation is a non-profit organization chartered to help military and overseas voters register and vote.

- In October 2007, Arel Cordero spoke on a panel at the inaugural Post-Election Audit Summit, which brought together policy makers, activists and academics to discuss and promote awareness of technical advances in election auditing. Arel spoke on the topic of transparency, particularly regarding random selection, and advocated simple, physical mechanisms over more intricate or computational means.

- ACCURATE PIs participated in threat modeling in Leon County, Florida.

- David Dill and Joe Hall testified before the California Secretary of State's "Post-Election Audit Standards Working Group" on July 2, 2007.

- Following up on his work as an election observer in Kazakhstan and Holland in 2005 and 2006, Douglas Jones attended a working meeting on "Election Observation and Electronic Voting" on March 22 and 23, 2007, convened by the Organization for Security and Cooperation in Europe Office for Democratic Institutions and Human Rights. This meeting brought together election observers, election administrators, and election activists from a number of OSCE member countries to discuss the problem of how to observe elections in which electronic voting is used.

- Douglas Jones's chapter in the IFES white paper "From Power Outages to Paper Trails" was distributed at the IFES Global Electoral Organization conference to election administrators and government officials from around the world.

- Douglas Jones served as a member of the Organization for Security and Cooperation in Europe Core Team for its Election Observing Mission for the Parliamentary Elections in Kazakhstan on August 18, 2007. The core team coordinates the activities of long-term observers and short-term observers and then drafts the report of the election-observing mission.

- Douglas Jones made presentations to the Post Election Audit Summit from October 25-27, 2007 in Minneapolis Minnesota. This summit brought together election administrators and activists to discuss what could be achieved from post-election audits. ACCURATE student Joseph Hall also presented, as did ACCURATE advisory board members Kim Alexander, Lillie Coney, Ron Rivest, Doug Kellner, Freddie Oakley, and (by video link) Deforest Soaries.

- Joseph Lorenzo Hall has been advising the New Hampshire Secretary of State's office as they begin to conduct research into methods of hand-counting. There is little experimental research that evaluates the various methods for hand-counting paper records, whether to tabulate votes or in the context of recounts and audits. The New Hampshire Secretary of State has designed an experimental research program that aims to answer some important questions related to counting team configuration, counting methods and voting technology for hand-counting.

- We continue to work on designing procedures for post-election audits in California. We've continued our work with San Mateo and Yolo Counties on designing detailed procedures that they can use to perform their post-election auditing as required by California law. We expect to publish a paper in early 2008 on the challenges associated with merging the scientific ideal of post-election audits with the practical constraints that election officials face. To extend this work, Joseph Lorenzo Hall will work with statistics Professor Philip Stark (UC Berkeley) and Kim Alexander (California Voter Foundation, ACCURATE affiliate) to conduct a pilot project in four California counties in 2008. Professor Stark has developed the state-of-the-art statistical method for auditing elections with the smallest sample necessary to confirm the results of a race to a specific level of confidence. In the pilot program, we will pilot this method for 1-2 local races, the data interchange and reporting protocols for races that span multiple jurisdictions and new ways to encourage the public to play an active role in this process.

- At the request of the San Francisco City & County Counsel's Office, we provided feedback on terms relating to source code disclosure in a contract that the city was negotiating with Sequoia Voting Systems. The final contract language closely reflects our suggestions, which, in turn, was based heavily on Joseph Lorenzo Hall's paper, *Transparency and Access to Source Code in Electronic Voting* (EVT 2006).

- Avi Rubin actively worked with officials in Maryland. He met with State Senator Kasemeyer, the second-highest ranking member of the state senate on February

19, in Annapolis to discuss electronic voting and potential new legislation. The same week, Avi Rubin also met with an attorney for the governor named Ralph Tyler for a similar discussion. Rubin reviewed and commented on draft state legislation about voting systems and testified on February 22, 2007 on Senate bill 392 in a hearing in the Maryland Senate. Rubin also testified in the Maryland House on the House version of the bill the same month.

- Avi Rubin led the technologists in a call between computer scientists and members of the Democratic National Committee in July, 2007, that was chaired by Phil McNamara. Rubin volunteered to assist in the reviewing of proposals for technology for the Michigan democratic primary, and Rubin also participated in several follow-up conference calls.

Post-Election Auditing and Analysis

ACCURATE members participated in analysis of several elections. Post-election audit is an important aspect of the election process, and one of the goals of the center is to help develop technologies that assist in the post-election audit process. This section describes some of the ACCURATE activities related to post-election audit and analysis.

- David Wagner participated in a post-election analysis of the November 2006 Congressional District 13 contest. The study, commissioned by the Florida State Division of Elections, examined the ES&S iVotronic voting machines used in Sarasota County, Florida, following a dispute over the outcome of that election. Observers had noted an anomalous rate of unvoted ballots in that race. The conclusion of that study was that the voting software did not cause or contribute to the high number of unvoted ballots.

- This summer, David Wagner led a study of three voting systems that are widely used in California and throughout the country, at the request of the California Secretary of State. Wagner was asked to lead a source code review and document review of these systems, and he recruited 25 faculty, including ACCURATE co-PI Dan Wallach, students, and industry experts to participate in the review. These reports constitute one of the most rigorous security reviews of these systems to date, and they revealed serious problems in all three systems examined. As a result, Secretary of State Debra Bowen de-certified several of the systems and instituted new procedural protections to mitigate or fix the other issues found during this review.

- The 2007 year saw increased adoption of a technique proposed by ACCURATE members Arel Cordero, David Dill, and David Wagner for selecting a random sample during post-election audits. Cordero, Dill, and Wagner proposed using 10-sided dice for transparent, verifiable random number selection. Several California counties have adopted this proposal. Also, ACCURATE members have worked with election officials in other counties to devise additional alternatives, so that election officials have more options to choose among.

Raising Awareness of Security, Testifying at Hearings, and Speaking in the Media
The ACCURATE center has had tremendous visibility in the media. Our co-PIs have been quoted on the front page of the New York Times, the Washington Post, the USA Today, on CNN, CSPAN, HBO, NPR, Time Magazine, Newsweek and in virtually every major media outlet. We have been the guests on the Diane Rehm Show, The Kojo Nnamdi Show, the Marc Steiner Show, and dozens of other radio programs around the country and the world. We have also served as major figures in several documentary films about electronic voting and security. ACCURATE co-PIs have given talks, including several keynote addresses, about electronic voting to the ACLU, the League of Woman Voters, and at many other organizations' events. The work of the ACCURATE co-PIs has raised the public awareness to the point where in the last two years, several states have passed laws requiring paper records of votes. Many other states are considering similar legislation, as is the federal government. Here are some details of specific activities of ACCURATE participants.

- David Wagner testified before the U.S. House of Representatives at a hearing of the Elections Subcommittee of the Committee on House Administration on March 15, 2007. The hearing was entitled "Election Reform: Machines & Software," and Wagner testified on technical and policy issues associated with public disclosure of voting system source code.

- David Wagner testified before the U.S. House of Representatives at a hearing of the Committee on Oversight and Government Reform, Subcommittee on Information Policy, Census, and National Archives on May 7, 2007. Wagner's testimony discussed the testing and certification of electronic voting systems.

- David Wagner served as an expert witness in the case Paralyzed Veterans of America v. Bruce McPherson, Secretary of State. The lawsuit challenges voting system certification decisions made by the California Secretary of State. Wagner served as an expert witness in support of the California Secretary of State.

- Douglas Jones wrote a letter to the Colorado legislature and Secretary of State on January 15, 2007 explaining the shortcomings of a move to all postal voting, after hearing that Colorado was considering such a move.

- Douglas Jones was quoted in Science News, the Chicago Tribune, the Tampa Tribune, the Sarasota Herald Tribune and the Miami Herald, and the San Jose Mercury News (Jan. 1, 2007), the Tampa Tribune (Feb. 15, 2007), Wired News (Apr 17, 2007), BBC News (Apr. 18, 2007), InfoWorld (Nov. 25, 2007).

- Peter Neumann participated in a multiyear study for the National Research Council Computer Science and Telecommunications Board Committee on Improving Cybersecurity Research in the United States. The completed report is entitled Toward a Safer and More Secure Cyberspace.

- Joseph Lorenzo Hall published the paper "Standards for e-Voting: The Work of

the Election & Voter Services Technical Committee" at the 2007 OASIS Symposium, available at: http://josephhall.org/papers/OS2007-EVS_TC.pdf

- Peter Neumann gave a written position paper and an oral briefing to a workshop on Voter Registration Databases for the Computer Science and Telecommunications Board (CSTB) as part of a study sponsored by the U.S. Election Assistance Commission.

- Both Avi Rubin and Peter Neumann appeared live on the Hugh Thompson show, and in subsequent productions on the AT&T Tech Channel.

- Avi Rubin produced several video taped lectures on electronic voting security issues in a professional studio at the National Center for State Courts at the William and Mary School of Law. The videos are available for online viewing and as part of the curriculum of an online course at http://icmeducation.org/electionlaw/modules.html.

- Joseph Lorenzo Hall testified before the Post-Election Audit Standards (PEAS) Working Group, convened by the California Secretary of State. His testimony was entitled "A Quick Review of Post-Election Audit Models" and is available at: http://josephhall.org/papers/20070702-PEAS-jhall.pdf

- Plenary Session: "Excellence in Election Verification," Tova Wang (chair), Toby Moore, Joseph Lorenzo Hall, Ion Sancho, 2nd Annual Election Verification Network Conference, EVN/Quixote Foundation (2007).

- Plenary Session: "Transparency in Post Election Audits," Lawrence Norden (chair), Ron Rivest, Joseph Lorenzo Hall, Arlene Ash, Howard Stanislevic, Post Election Audit Summit; American Statistical Association/Verified Voting Foundation/NYU Brennan Center for Justice/Common Cause/Citizens for Election Integrity Minnesota/The Florida Voters Coalition (2007), available at: http://www.josephhall.org/papers/20071025-PEAS-jhall.pdf

- Plenary Session: "2006 Year in Review: Developments in Electronic Voting Research," Pam Smith (chair), John Bonifaz, Aaron Burstein Barbara Burt, 2nd Annual Election Verification Network Conference Developments in 2006," EVN/Quixote Foundation (2007).

- Aaron J. Burstein presented an "Overview of the Brennan Center/Samuelson Clinic Report on Post-Election Auditing" at the Election Verification Network August, 2007 teleconference.

- Peter Neumann organized and chaired a session on voting integrity at the 2007 Conference on Computers, Freedom, and Privacy, Montreal CANADA, May 3, 2007. Panelists included Lillie Coney, Doug Jones, and Barbara Simons. He also keynoted the IEEE Security and Privacy at the Claremont in Berkeley/Oakland on

May 21, 2007, *Reflections on the Future of Security and Privacy*, with emphasis on voting system integrity.

- Dan Wallach spoke at several government functions, including testimony before the United States Senate Committee on Rules and Administration and the Tennessee Advisory Committee on Intergovernmental Relations (TACIR). Wallach also gave invited talks in Belgium, Chile and Germany, as well as an ABA continuing legal education panel in San Francisco.

- Avi Rubin testified at a hearing of the US House Appropriations Committee on March 7, 2007. He also spent an hour meeting with Congressman Vernon Ehlers of Michigan to discuss electronic voting and provided feedback to the Congressman about a public report that Rep. Ehlers was interested in.

- Dan Wallach gave a talk entitled *Real-world Electronic Voting* to the 2007 National Lawyers Council National Leadership Convention and at the Claim Democracy Conference in Washington in November, 2007.

Summary and Future Plans

ACCURATE is grateful to the National Science Foundation for their funding and support of our activities. As this annual report shows, the center has been very active in research, education, and outreach, and the far-reaching impact is apparent to everyone in the elections community. It is our plan to continue our activities on all fronts and to help make our democracy more secure, reliable, usable, auditable and transparent, while advancing the state of the art in computer security, cryptography, systems usability and accessibility, and technology policy. The 2008 election will provide ACCURATE a chance to contribute on many different levels. Our center has already had an impact on the upcoming election, and we will continue to work to make this election season as successful as possible, and to maximize the lessons we can learn from it.

More information about ACCURATE can be found on our center web site at http://accurate-voting.org.

Appendix A

Principal Investigators

- **Aviel D. Rubin** (Director) Department of Computer Science , Johns Hopkins University, rubin@cs.jhu.edu: http://www.cs.jhu.edu/~rubin/

- **Dan S. Wallach** (Associate Director) Department of Computer Science, Rice University, dwallach@cs.rice.edu: http://www.cs.rice.edu/~dwallach/

- **Dan Boneh** Department of Computer Science , Stanford University, dabo@cs.stanford.edu: http://crypto.stanford.edu/~dabo/

- **Michael D. Byrne** Department of Psychology, Rice University, byrne@rice.edu: http://chil.rice.edu/byrne/

- **David L. Dill** Department of Computer Science, Stanford University, dill@cs.stanford.edu: http://verify.stanford.edu/dill/

- **Douglas W. Jones** Department of Computer Science , University of Iowa, jones@cs.uiowa.edu, http://www.cs.uiowa.edu/~jones/

- **Peter G. Neumann** Computer Science Laboratory , SRI International, neumann@csl.sri.com: http://www.csl.sri.com/users/neumann/neumann.html

- **Deirdre Mulligan** School of Law , University of California, Berkeley, dmulligan@law.berkeley.edu: http://law.berkeley.edu/faculty/profiles/facultyProfile.php?facID=1018

- **David A. Wagner** Department of Computer Science, University of California, Berkeley , daw@cs.berkeley.edu: http://www.cs.berkeley.edu/~daw/

- **Brent Waters** Computer Science Laboratory , SRI International, bwaters@csl.sri.com: http://www.csl.sri.com/users/bwaters/

Appendix B

External Advisory Board

- **Kim Alexander** — Ms. Alexander is president and founder of the California Voter Foundation (CVF), a nonprofit, nonpartisan organization dedicated to advancing the responsible use of technology in the democratic process.

- **Secretary Debra Bowen** — Debra Bowen was elected to be California's 30th Secretary of State on November 7, 2006, making her only the sixth woman elected to a statewide constitutional office since California was admitted to the Union in 1850. Born in Rockford, Illinois, Bowen graduated from Michigan State University in 1976 and earned her law degree from the University of Virginia in 1979. In 1984, she started her own California law firm specializing in small business start-ups, tax law, land use, and environmental issues. Her long history of community activism began in the 1980's when she became involved with her local Neighborhood Watch program. Bowen was elected to represent the 53rd Assembly District in 1992 and served three two-year terms before being elected to represent the 28th Senate District in 1998. Bowen served two four-year terms in the Senate before she was elected as California's Secretary of State.

- **Lillie Coney** — Ms. Coney is Associate Director with the Electronic Privacy Information Center (EPIC). Her issue areas include nanotechnology, surveillance, children's privacy, civil rights and privacy, coalition development, spectrum, census, and electronic voting.

- **Edward W. Felten** — Dr. Felten is Professor of Computer Science and Public Affairs at Princeton University, and is the founding Director of Princeton's Center for Information Technology Policy. His research interests include computer security and privacy, especially relating to media and consumer products; and technology law and policy. He has published about eighty papers in the research literature, and two books. His research on topics such as web security, copyright and copy protection, and electronic voting has been covered extensively in the popular press. His weblog, at freedom-to-tinker.com, is widely read for its commentary on technology, law, and policy. He was the lead

computer science expert witness for the Department of Justice in the Microsoft antitrust case, and he has testified in other important lawsuits. He has testified before the Senate Commerce Committee on digital television technology and regulation, and before the House Administration Committee on electronic voting. In 2004, Scientific American magazine named him to its list of fifty worldwide science and technology leaders.

- **David Jefferson** — Dr. Jefferson has been conducting research at the intersection of computers, the Internet, and public elections for over a decade. He is Chair of the California Secretary of State's Voting systems Technical Assessment and Advisory Board, which provides technical advice on the security, privacy, and reliability of voting systems.

- **Doug Kellner** — Mr. Kellner is Co-Chair of the New York State Board of Elections. He has served as one of the ten commissioners of the New York City Board of Elections since 1993. Before he became commissioner, Mr. Kellner was the election lawyer for the Democratic Party in Manhattan and played major roles in election-related decisions and procedural-drafting in New York City.

- **David Klein** — David Klein is the Elections Research & Operations Specialist at the Ohio Office of Secretary of State. His responsibilities include evaluating expert scientific, analytic, and technical information to advance Secretary Jennifer Brunner's goal of restoring trust in Ohio's elections by ensuring that they are fair, honest, and accurate. Prior to joining the Ohio Office of Secretary of State, Dave was involved in a variety of operations and technology management projects, including the development of standard practices and policies; implementation of technical systems; and the improvement of testing methods and analytics. He is a graduate of The University of Texas at Austin, where he received his B.A. in Psychology. After completing his undergraduate work, Dave continued his studies at The Ohio State University, earning an M.A. in Social Psychology and a Ph.D./ABD in Social Neuroscience under a National Science Foundation Fellowship award.

- **Sharon Laskowski** — Dr. Sharon Laskowski is a computer scientist in the Information Technology Laboratory of the National Institute of Standards and

Technology and manager of the Visualization and Usability Group, which is developing evaluation methods, metrics, and standards for human-computer interaction. She was the lead author of the report "Improving the Usability and Accessibility of Voting Systems and Products" as mandated in the Help America Vote Act (HAVA) of 2002, Public Law 107-252. Dr. Laskowski provides technical and research assistance to the Technical Guidelines Development Committee (TGDC). She leads the effort to develop the usability, accessibility and privacy requirements for the Voluntary Voting System Guidelines.

- **Scott Luebking** — Mr. Luebking is a usability and accessibility expert that has worked closely with California jurisdictions to educate their staff about the importance of usability and accessibility assessment for voting system evaluation and procurement.

- **Freddie Oakley** — Since 1999, Ms. Oakley has served as the Chief Deputy Clerk/Recorder for Yolo County, California. In addition to managing elections, she has implemented a plan to ensure privacy and security of Recorder-maintained documents, worked to incorporate the latest technology into both the Elections and Recorder processes and created a successful Junior Voter Program.

- **Ron Rivest** is a professor of computer science at MIT. He is co- inventor of the famous RSA algorithm, creator of MD5 and one of the world's most renowned cryptographers. Professor Rivest is a recipient of the ACM Turing Award, the highest prize in computer science. Dr. Rivest is a member of the EAC's TGDC.

- **Noel Runyan** has over thirty-six years experience with microprocessors, digital logic, analog circuits, speech output, systems architecture, human interface design, and development of access technology for persons with disabilities. He has extensive experience with the development and application of speech and braille interface technologies and integration of computer systems with speech, braille, and/or large print output. He founded Speech Works in 1983, which was renamed Personal Data Systems in 1985, to develop communications devices for persons with visual impairments. In addition, Mr. Runyan has designed and developed hardware and software for the Audapter speech synthesizer and the

Talking Tablet System as well as authored the EasyScan, BuckScan and PicTac scanning programs. [Noel Runyan was a coauthor with Jim Tobias of the California Top-To-Bottom-Review on accessibility.]

- **Dr. DeForest B. Soaries, Jr.** is the Senior Pastor of the First Baptist Church of Lincoln Gardens in Somerset, New Jersey. Highlights of Dr. Soaries' work include recruiting 265 families to become foster parents to 325 abandoned babies; helping 140 children find adoptive parents; constructing 124 new homes for low and moderate income residents to own; creating the first faith based Cisco Technology Academy in the country; operating the Central New Jersey STRIVE program for job readiness; serving hundreds of youth in an after school center and homework club; forming a youth entrepreneurship program; and redeveloping commercial real estate. Dr. Soaries is also the former Chairman of the United States Election Assistance Commission and was appointed by President George W. Bush on December 15, 2003 after being confirmed by the United States Senate. In February 2003, Dr. Soaries was appointed to be a public director of the Federal Home Loan Bank of New York. He was a member of the affordable housing committee of the bank. From January 12, 1999 to January 15, 2002, Dr. Soaries served as New Jersey's Secretary of State. Dr. Soaries earned a Bachelor of Arts Degree from Fordham University; a Master of Divinity Degree from Princeton Theological Seminary; and a Doctor of Ministry Degree from United Theological Seminary. He has also received six honorary Doctorate degrees from institutions of higher learning.

- **Anthony Stevens** — Mr. Stevens is Assistant Secretary of State for New Hampshire, a position he has held since 1994. In this role, he has served as the New Hampshire Coordinator for the Help America Vote Act and Project Manager for the Statewide Voter Registration System. He is also a member of the EAC's Standards Board. Prior to his current position, he was Vice President for Corporate Lending at Citibank and a member of the New Hampshire state legislature for two terms.

Appendix C

ACCURATE Publications

2008

Conferences

- Sarah P. Everett, Kristin K. Greene, Michael D. Byrne, Dan S. Wallach, Kyle Derr, K., Dan Sandler, and T. Torous, (2008, in press). Is newer always better? The usability of electronic voting machines versus traditional methods. To appear in *Human Factors in Computing Systems: Proceedings of CHI 2008*.

2007

Books

- Peter G. Neumann, *Reflections on Trustworthy Systems.* Advances in Computers, Volume 70, edited by Marvin Zelkowitz, Academic Press.

- Peter G. Neumann, *The Future of Information Assurance.* Final chapter of the Computer Security Handbook, fifth edition, Wiley, 2008, accepted.

Journals

- Matt Bishop and David Wagner, Risks of E-voting. *Communications of the ACM*, 50, 11, November 2007, Inside Risks column (Peter G. Neumann, editor). This is a summary of the California Top-To-Bottom Review.

Conferences

- Ka-Ping Yee. Extending Prerendered-Interface Voting Software to Support Accessibility and Other Ballot Features. *Proceedings of the 2nd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07)*, 2007.

- Joseph Lorenzo Hall, Contractual Barriers to Transparency in Electronic Voting. *Proceedings of the 2nd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07)*, 2007. available at: http://josephhall.org/papers/jhall_evt07.pdf

- Ryan Gardner, Sujata Garera, and Aviel D. Rubin. On the Difficulty of Validating Voting Machine Software with Software. *Proceedings of the 2nd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07)*, 2007.

- Stephen N. Goggin and Michael D. Byrne. An Examination of the Auditability of Voter Verified Paper Audit Trail (VVPAT) Ballots. *Proceedings of the 2nd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07)*, 2007.

- Sujata Garera and Aviel D. Rubin, An Independent Audit Framework for Software Dependent Voting Systems. *14th ACM Conference on Computer and Communications Security*, November, 2007.

- Joseph L. Hall. Contractual Barriers to Transparency in Electronic Voting. In *Proceedings of the 2nd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07)*, 2007.

- Daniel Sandler and Dan S. Wallach. Casting Votes in the Auditorium. In *Proceedings of the 2nd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07)*, 2007.

- Ka-Ping Yee. Extending Prerendered-Interface Voting Software to Support Accessibility and Other Ballot Features. In *Proceedings of the 2nd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07)*, 2007.

- John Bethencourt, Dan Boneh, and Brent Waters, Cryptographic Methods for Storing Ballots on a Voting Machine. *The 14th Annual Network & Distributed System Security Conference (NDSS 2007)*.

- John Bethencourt, Amit Sahai, and Brent Waters, Ciphertext-Policy Attribute-Based Encryption. *Proceedings of 2007 IEEE Symposium on Security and Privacy*. http://www.csl.sri.com/users/bwaters/publications/papers/cp-abe.pdf

- John Bethencourt, Dawn Song and Brent Waters, Analysis-Resistant Malware. *15th Annual Network & Distributed System Security Conference (NDSS 2008)*.

- Xavier Boyen and Brent Waters, Full-Domain Subgroup Hiding and Constant-Size Group Signatures. *Proceedings of 10th Workshop in Practice and Theory of Public Key Cryptography (PKC 2007)*. (Won best paper award)

- Byrne, M. D., Greene, K. K., & Everett, S. P. (2007). Usability of voting systems: Baseline data for paper, punch cards, and lever machines. *Human Factors in Computing Systems: Proceedings of CHI 2007* (pp. 171-180). New York: ACM.

- Goggin, S., & Byrne, M. D. (2007). An examination of the auditability of voter verified paper audit trail (VVPAT) ballots. *Proceedings of the 2007 USENIX/ACCURATE Electronic Voting Technology Workshop*.

- Alex Halderman and Brent Waters Harvesting Verifiable Challenges from Oblivious Online Sources. *Proceedings of 14th ACM Conference on Computer and Communications Security (CCS 2007)*, 2007. http://www.csl.sri.com/users/bwaters/publications/papers/combine2007.pdf

- Rafail Ostrovsky, Amit Sahai, and Brent Waters, Attribute-Based Encryption with Non-Monotonic Access Structures. *Proceedings of 14th ACM Conference on Computer and Communications Security (CCS 2007)*. http://eprint.iacr.org/2007/323.pdf

- Dan Boneh and Brent Waters, Conjunctive, Subset, and Range Queries on Encrypted Data. *The Fourth Theory of Cryptography Conference (TCC 2007)*

- Hovav Shacham and Brent Waters, Efficient Ring Signatures without Random Oracles. *Proceedings of 10th Workshop in Practice and Theory of Public Key Cryptography (PKC 2007)*. http://eprint.iacr.org/2006/289.pdf

Reports

- Ka-Ping Yee. Report on the Pvote security review. November 14, 2007.

- Lawrence Norden, Aaron Burstein, Joseph Lorenzo Hall and Margaret Chen, Post-Election Audits: Restoring Trust In Elections; Brennan Center for Justice at New York University School of Law and the Samuelson Law, Technology & Public Policy Clinic at the University of California, Berkeley School of Law

(Boalt Hall). available at:
http://www.brennancenter.org/dynamic/subpages/download_file_50135.pdf

- Joseph Lorenzo Hall and Laura Quilter, Documentation Review of The Hart Intercivic System 6.2.1 Voting System.; University of California for the California Secretary of State's Top-To-Bottom Review of Voting Systems. available at:
http://www.sos.ca.gov/elections/voting_systems/ttbr/hart_doc_final.pdf

- Aaron J. Burstein, Nathan S. Good and Deirdre K. Mulligan, Review of the Documentation of the Sequoia Voting System; University of California for the California Secretary of State's Top-To-Bottom Review of Voting Systems. available at:
http://www.sos.ca.gov/elections/voting_systems/ttbr/sequoia_doc_final.pdf

- Patrick McDaniel, Matt Blaze, Giovanni Vigna, Adam Aviv, Davide Balzarotti, Greg Banks, Kevin Butler, Pavol Cerny, Sandy Clark, Marco Cova, Eric Cronin, William Enck, Viktoria Felmetsger, Joseph Lorenzo Hall. Harri Hursti, Richard Kemmerer, Steve McLaughlin, Laura Quilter, William Robertson, Gaurav Shah, Micah Sherr, Patrick Traynor, Fredrik Valeur, EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing. Ohio Secretary of State's EVEREST Review of Voting Systems

- Joseph A. Calandrino, Ariel J. Feldman, J. Alex Halderman, David Wagner, Harlan Yu, William P. Zeller. Source Code Review of the Diebold Voting System. July 20, 2007. Report commissioned as part of the California Secretary of State's Top-To-Bottom Review of California voting systems.

- Srinivas Inguva, Eric Rescorla, Hovav Shacham, and Dan S. Wallach. Source Code Review of the Hart InterCivic Voting System. July 20, 2007. Report commissioned as part of the California Secretary of State's Top-To-Bottom Review of California voting systems.

- Matt Blaze, Arel Cordero, Sophie Engle, Chris Karlof, Naveen Sastry, Micah Sherr, Till Stegers, Ka-Ping Yee. Source Code Review of the Sequoia Voting System. July 20, 2007. Report commissioned as part of the California Secretary of State's Top-To-Bottom Review of California voting systems.

- Joseph Lorenzo Hall, Laura Quilter. Documentation Review of the Hart InterCivic System 6.2.1 Voting System. July 20, 2007. Report commissioned as part of the California Secretary of State's Top-To-Bottom Review of California voting systems.

- Aaron J. Burstein, Nathan S. Good, Deirdre K. Mulligan. Review of the Documentation of the Sequoia Voting System. July 20, 2007. Report commissioned as part of the California Secretary of State's Top-To-Bottom Review of California voting systems.

- Ka-Ping Yee. Pvote Software Review Assurance Document. March 29, 2007.

- David L. Dill and Dan S. Wallach, "Stones Unturned: Gaps in the Investigation of Sarasota's Disputed Congressional Election," April 2007. Available at http://www.cs.rice.edu/~dwallach/pub/sarasota07.html

- Alec Yasinsac, David Wagner, Matt Bishop, Ted Baker, Breno de Medeiros, Gary Tyson, Michael Shamos, and Mike Burmester. Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware. February 23, 2007. Report commissioned by the Florida State Division of Elections.

- Alec Yasinsac, David Wagner, Matt Bishop, Ted Baker, Breno de Medeiros, Gary Tyson, Michael Shamos, and Mike Burmester. Machine Firmware. February 23, 2007. Report commissioned by the Florida State Division of Elections.

- Peter G. Neumann, Security and Privacy Risks in Voter Registration Databases (VRDBs), prepared for a Workshop on Voter Registration Databases, November 29-30, 2007, organized by the National Academies' Computer Science and Telecommunications Board (CSTB) as part of a study sponsored by the U.S. Election Assistance Commission. http://www.csl.sri.com/neumann/cstb-vrdb07

Other

- Sara P. Everett. (2007). The Usability of Electronic Voting Machines and How

Votes Can Be Changed Without Detection. Doctoral dissertation, Rice University, Houston, TX.

- Craig Gentry, Chris Peikert and Vinod Vaikuntanathan, Trapdoors for Hard Lattices and New Cryptographic Constructions, In submission.

- Aaron Burstein and Joseph Lorenzo Hall, Unlike Ballots, EAC Shouldn't Be Secretive. *Roll Call*, 22 January, (2007). available at: http://josephhall.org/papers/Burstein_Hall-Roll_Call_2007-01-26.pdf

2006

Books

- Aviel D. Rubin, *Brave New Ballot: The Battle to Safeguard Elections in the Age of Electronic Voting,* Random House, September, 2007.

Journals

- Peter G. Neumann, Holistic Systems, *ACM Software Engineering Notes*, 13,6, November 2006, pp. 4–5.

Conferences

- Peter G. Neumann, System and Network Trustworthiness in Perspective, invited paper for keynote talk, *Proceedings of the ACM Computer-Communication Security Conference*, Alexandria VA, October-November 2006, pp. 1-5.

- Peter G. Neumann, Risks of Untrustworthiness, invited Classic Papers Track, *Proceedings of the IEEE 22nd Annual Computer Security Application Conference (ACSAC)*, Miami Beach, December 13-14, 2006. pp. 321–326.

- Douglas W. Jones, Technologists as Political Reformers: Lessons from the Early History of Voting Machines presented at the Society for the History of Technology annual conference, Las Vegas, October 13, 2006.

- Crutchfield, C., Molnar,D., & Turner,D. (2006) Approximate Measurement of Voter Privacy Loss in an Election With Precinct Reports. Presented at NIST/NSF Voting Systems Rating Workshop.

- Kristin K. Greene, Michael D. Byrne, and Sarah P. Everett. (2006). A comparison of usability between voting methods. In *Proceedings of the 2006 USENIX/ACCURATE Electronic Voting Technology Workshop*.

- Sarah P. Everett, Michael D. Byrne, and Kristin K. Greene. (2006). Measuring the usability of paper ballots: Efficiency, effectiveness, and satisfaction. *Proceedings of the Human Factors and Ergonomics Society 50th Annual Meeting*, (pp. 2547-2551). Santa Monica, CA: Human Factors and Ergonomics Society.

- Arel Cordero, David Wagner, David Dill. The Role of Dice in Election Audits – Extended Abstract. *IAVoSS Workshop On Trustworthy Elections*, 2006.

- Ka-Ping Yee, David Wagner, Marti Hearst, and Steven Bellovin. Prerendered User Interfaces for Higher-Assurance Electronic Voting. In *Proceedings of the 2006 USENIX/ACCURATE Electronic Voting Technology Workshop*, 2006.

- Douglas W. Jones, and Tom C. Bowersox. Secure Data Export and Auditing using Data Diodes. In *Proceedings of the 2006 USENIX/ACCURATE Electronic Voting Technology Workshop*, 2006.

- Naveen Sastry, Tadayoshi Kohno, and David Wagner. Designing voting machines for verification. In *Proceedings of the 2006 USENIX/ACCURATE Electronic Voting Technology Workshop* (August 4, 2006).

- Dan Boneh and Brent Waters, A Fully Collusion Resistant Broadcast, Trace and Revoke System. *Proceedings of 13th ACM Conference on Computer and Communications Security (CCS 2006)*

- Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters, Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. *Proceedings of 13th ACM Conference on Computer and Communications Security (CCS 2006)*.

- Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters, Secure

Attribute-Based Systems. *Proceedings of 13th ACM Conference on Computer and Communications Security (CCS 2006).*

- David Molnar, Tadayoshi Kohno, Naveen Sastry, and David Wagner. Tamper-Evident, History-Independent, Subliminal-Free Data Structures on PROM Storage -or- How to Store Ballots on a Voting Machine (Extended Abstract). In *Proceedings of IEEE Symposium on Security and Privacy* (May 21-24, 2006).

Reports

- Paula Hawthorn, Barbara Simons, Chris Clifton, David Wagner, Steven M. Bellovin, Rebecca N. Wright, Arnon Rosenthal, Ralph Spencer Poore, Lillie Coney, Robert Gellman, Harry Hochheiser. Statewide Databases of Registered Voters: Study Of Accuracy, Privacy, Usability, Security, and Reliability Issues. February 16, 2006. Study commissioned by the U.S. Public Policy Committee of the Association for Computing Machinery.

- David Wagner, David Jefferson, Matt Bishop, Chris Karlof, Naveen Sastry Security Analysis of the Diebold AccuBasic Interpreter. Report of the California Secretary of State's Voting Systems Technology Assessment Advisory Board (VSTAAB), February 14, 2006.

2005

Reports

- Matt Bishop, Loretta Guarino, David Jefferson, David Wagner. Analysis of Volume Testing of the AccuVote TSx/AccuView. Report of the California Secretary of State's Voting Systems Technology Assessment Advisory Board (VSTAAB), October 11, 2005.