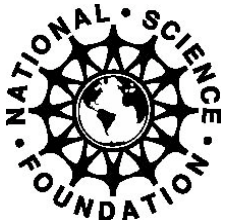
ACCURATE: A Center for Correct Usable Reliable Auditable and Transparent Elections

2008 Annual Report



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

Overview

2008 was a particularly good year for ACCURATE. Given the importance of the Presidential election and the amount of attention the election received, ACCURATE members had opportunities to serve in many capacities. We worked as poll workers, served on government panels, studied and analyzed real voting systems, and contributed to the election process in several other ways. Our outreach activities included working with several boards of elections, secretaries of state, and organizations such as the Carter center to help them understand the technology issues that they faced. We provided feedback to the Election Assistance Commission on their proposed standards, and involved people like Debra Bowen, the Secretary of State of California and Tom Wilkie, the executive director of the EAC, in our workshops.

This 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. One highlight of our year was the work on the VoteBox system, an experimental voting system developed at Rice University. VoteBox is an excellent platform for examining system-architecture issues, as well as for studying the application of cryptographic and other verification techniques. In addition, it allowed for interesting human factors studies to research the interaction between voters and the voting machinery – a much overlooked area with significant implications in real elections.

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, NBC, ABC News and 20/20 as well as many other media outlets.

Co-PI David Dill co-chaired the Electronic Voting Technology (EVT) 2008 workshop, together with Tadayoshi Kohno. EVT is an annual workshop co-sponsored by ACCURATE and by USENIX. The EVT 2008 workshop was phenomenally successful. We received 34 submissions and accepted 15 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 as a large number of papers at EVT 2008 were authored by many researchers, including both researchers affiliated with ACCURATE and many researchers not affiliated with ACCURATE. We noticed many attendees from disciplines other than computer science, in particular there was very strong participation from election officials at the local, state and national levels. Plans for EVT 2009 are underway; it will be co-chaired by ACCURATE's Joseph Lorenzo Hall and ACCURATE advisor David Jefferson.

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 25 graduate students, 19 undergraduates, two law students, and two post-docs.

Finally, our center advisory board welcomed a new member, Barbara Simons, former President of the ACM. A complete list of our external advisory board can be found in Appendix B of this report.

Detailed Activities

This section provides details on the 2008 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.

- At the University of Iowa, Douglas Jones, Paul Cotton and Mark Slayton are working on relating information from event logs in touch-screen voting machines to human-factors problems in the voting machine interface. This work was inspired by Jones' observation that post-election audits conducted using hand-marked paper ballots routinely reveal the human-factors problems present in the design of those ballots, but that post-election auditing of DRE machines has not generally revealed anything about these problems. We note that event log entries recording duration of screen touch, attempts to change votes in a race, and returns to a race from the summary screen can be made without introducing violations of the voter's right to a secret ballot. We hypothesize that we will be able to detect touch-screen calibration problems, touch-screen sensitivity problems, and banner blindness from an event log in which these details are recorded. We are currently modifying the Pvote system to provide a platform for this experiment.

- At Rice University, Dan Wallach and Daniel Sandler, along with a number of

talented Rice undergraduate students, have built a complete (albeit prototype) touch-screen electronic voting system called "VoteBox." VoteBox has demonstrated how a variety of cryptographic techniques, such as homomorphic cryptosystems and immediate ballot challenging, can be integrated into an implementation with local network storage, replicating data everywhere and giving detailed opportunities for auditing the results to ensure that failures are not only caught but are more likely to be correctable. VoteBox also has allowed us to experiment with how to effectively support remote voting (e.g., from overseas military bases). VoteBox serves as a platform for examining system-architecture issues, as well as for studying the application of cryptographic and other verification techniques. VoteBox also serves as research infrastructure for human factors testing (performed by Mike Byrne's group, described below). VoteBox is now available as an open-source software distribution (votebox.cs.rice.edu).

- Last summer, David Wagner helped to lead the California Top-To-Bottom Review of California's voting systems, at the request of California Secretary of State Debra Bowen. This year, Wagner collaborated with several other researchers involved in the Top-To-Bottom Review to study what lessons can be learned from that review. In particular, they proposed a number of procedural and technical mitigations designed to protect existing voting systems against the most serious security risks identified in the Top-To-Bottom Review. A core premise of this work is that it is difficult and expensive to make major changes to deployed voting system software and hardware, so it makes sense to look for mitigations that can be applied to existing systems. Their paper, titled "You Go to Elections with the Voting System You Have: Stop-Gap Mitigations for Deployed Voting System", was published at the 2008 USENIX/ACCURATE Electronic Voting Workshop.

- At UC Berkeley, Arel Cordero and David Wagner completed their work on improving voting system audit logs. This work was motivated by Wagner's involvement in a prior voting system audit, where Wagner discovered that the existing audit logs were missing some information that would have been useful in the investigation. Cordero and Wagner's recent research contemplates how to extend existing DRE voting machines to produce detailed information about everything that each voter saw and did while interacting with the voting machine, which might help an election investigator discern voter intent or diagnose some kinds of systematic problems. This work was published at the 2008 USENIX/ACCURATE Electronic Voting Workshop.

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:

- At Stanford, Eric Smith and David Dill (with advice from Dan Boneh) have developed fully automatic methods for proving the correctness of block cipher

implementations. This method checks the equivalence of two descriptions of an algorithm. One of those descriptions can be an implementation in a programming language (in this case, Java) and the other can be either an implementation or a specification in a functional language. The method "unrolls" the programs into a single large expression, which is possible because the loops in block ciphers only iterate up to a known maximum number of times, uses testing with random inputs to find sub-expressions that are equivalent for all test inputs, and then generates a collection of theorems to be proved showing that subexpressions that never differ for tests are actually equivalent. The theorems are proved automatically by simplification and, if necessary, reducing to a propositional logic formula that is solved using efficient off-the-shelf libraries to solve the propositional logic satisfiability problem (SAT). This method has been used to prove that most of the Java implementations of block ciphers in the widely-used "Bouncy Castle" and Sun Java crypto provider are equivalent to their IFIP specifications. The only manual effort required is to wrap the implementations in a small amount of "driver code" that sets up the key and message values for the cipher implementation.

- We continue to develop new cryptographic systems that can help secure voting systems. Last year we developed new signature schemes (so called append-only signatures) that prevent tampering with stored votes. This year we focused on new encryption primitives that can help protect voter privacy. For example, we developed a new identity-based encryption system that does not use algebraic geometry (previous efficient systems used it heavily). The paper won a best paper award where it was presented (FOCS'07). We also constructed an encryption scheme that remains secure in the presence of encryption cycles. As a third example, we developed a privacy-preserving identification scheme that is provably free of covert channels.

- At Johns Hopkins, Avi Rubin, Ryan Gardner and Sujata Garera examined the issue of voter coercion in a voting scheme published by Josh Benaloh. To address attacks such as ours, we provided a formal definition of coercion resistance for end-to-end voting. We designed a new scheme, extended from Benaloh's, that is provably coercion resistant. In addition to providing accuracy and coercion resistance, our scheme emphasizes ease-of-use for the voter.

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.

- At UC Berkeley, Cynthia Sturton and David Wagner are in the process of collaborating with Sanjit Seshia and Susmit Jha, two experts in formal methods, to investigate novel approaches to design for verification. They are building a

bare-bones voting machine that can be formally verified using model checking and satisfiability checking. This project espouses a twin philosophy of "design for verification" (where the system is designed from the start to enable formal verification of its correctness) as well as "design for testability" (where the system is designed so that pre-election testing will be maximally effective). One novel aspect of this work is that they are implementing the voting machine in hardware; this eliminates the need to rely upon (or formally verify) an operating system, compiler, or system libraries.Another interesting aspect of this work is that it identifies conditions under which systematic testing of the voting machine can provide strong assurance that the voting machine will behave correctly and is free of configuration errors and logic bugs. This is work in progress.

- A team of students at UC Berkeley recently completed work on tools and languages for verifying that code will behave in a functionally pure way. This work was initially inspired by work on voting machines, where the goal was to demonstrate that votes recorded on election day would be interpreted by a central tabulator in the same way that they were initially prepared by the voting machine. However, we soon recognized that these techniques were of broader applicability to a number of problems in computer security, leading to a publication that examined many computer security applications of verification of functional purity and proposed ways that a language could enable such verification. This represents an example of a phenomenon we predicted in the original proposal: while the ACCURATE center is focused on improving voting technology, many elements of our work may have spin-off benefits in other areas of computer security and computer science. This work was published at the 15th ACM Conference on Computer and Communication Security (ACM CCS 2008).

- At Johns Hopkins, Avi Rubin, Ryan Gardner and Sujata Garera designed and implemented a system for allowing a poll worker to verify that the code running on a voting machine has not changed. The system works by allowing the poll worker to provide a random challenge (perhaps via a scratch-off card) to the machine. The machine then computes a function of a checksum of the code it is running in such a way that the only way to produce a correct response to the challenge within a particular time window is for the correct code to be running. The system utilizes the fact that memory accesses from cache are much faster than other main memory hits. Computing the correct checksum on the wrong code causes cache misses, so the poll worker, armed with correct challenge response pairs, a time value, and a stopwatch, can validate that the correct code is on the voting machine. Future work will involve removing some of the assumptions that were required to achieve this.

Relating Policy to Technology

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

- Douglas Jones has continued to work with the Organization for Security and Cooperation in Europe on their methodology for observing elections in which electronic voting is used. Current drafts of this methodology have strong implications for voting system standards in OSCE member countries, including the United States.

- Dan Wallach authored a paper, "Voting System Risk Assessment via Computational Complexity Analysis," which considered a variety of different techniques for how to quantify whether one voting system is more less secure than another one, and settles on computational complexity ("big-O" notation) as a flexible and powerful way of making distinctions between different voting technologies.

- David Wagner led a security review of the Scytl Pnyx.core ODBP voting system, working in collaboration with a team of five other computer scientists. This review was commissioned by the Florida Department of State. The Scytl Pnyx.core ODBP voting system is a remote voting system, designed to enable overseas voters and military voters to vote in US elections from polling places set up abroad. This security review was used as part of the Florida Department of State's certification process for the Scytl voting system.

- Aaron Burstein and Joseph Lorenzo Hall prepared and submitted, on behalf of ACCURATE, comments to the U.S. Election Assistance Commission (EAC) on the draft of the next generation of Voluntary Voting System Guidelines (VVSG). Once adopted by the EAC, the new VVSG will provide federal guidelines for electronic voting system equipment, documentation, and testing. Though states may choose not to require that their voting systems conform to the VVSG, the vast majority of states will do so. Thus, the VVSG—in whatever form they finally take—will become a de facto national standard for electronic voting systems. ACCURATE's comments laud the new draft as a groundbreaking and badly needed overhaul of our national voting system standards while making constructive suggestions for further development. The most significant element of the draft VVSG is the requirement for software independence. ACCURATE fully supports requiring software independence as the backbone of a robust and comprehensive next-generation voting system certification regime. The commentary goes on to emphasize the importance of welcome features of the draft: adversarial vulnerability testing, volume testing, the new framework for usability and accessibility testing and comprehensive voting system documentation requirements. The VVSG draft also leverages a relationship with the EAC's certification authority and its voting system test lab standards to bring much needed transparency to the testing process. The comment closes by pointing out areas of the VVSG that will require increased institutional support outside of the VVSG process, including the crucial innovation class and closing the loop for incident reporting and feedback. Since its inception, ACCURATE's public comments in a range of forums have argued for these changes on technical, usability, and public policy grounds.

Accordingly, our comments on the VVSG draft were strongly supportive, and we will file reply comments once the EAC issues its response to the first round of public comments.

- A team of ACCURATE researchers, including David Dill, David Wagner, Aaron Burstein, Arel Cordero and Joseph Lorenzo Hall, were invited by San Mateo County, California to help them revise the procedures they use for their audit. This multi-year endeavor started with meetings in 2006 and 2007 that culminated with an iterative redesign of San Mateo's post-election manual tally (audit) procedures. Hall authored an initial set of procedures used in the November 2007 election and then revised them based on observations and feedback for the 2008 election cycle. Hall also developed a dice-binning tool to make random audit selection with 10-sided dice (pioneered by Cordero, Dill and Wagner in 2005) more efficient. The resultant procedures, software and a peer-reviewed academic paper were presented and published at the 2008 USENIX/ACCURATE Electronic Voting Technology conference.

- We have undertaken a significant expansion of our prior work on contractual barriers to transparency in voting systems. As that work showed, the contracts between voting system manufacturers and election jurisdictions typically contain severe restrictions on jurisdictions' ability to analyze their systems and to disclose information to the public about them. But these contracts go much further in regulating the use and understanding of electronic voting systems. They govern contingencies concerning certification, they provide guarantees (and disclaimers) concerning system security, and they govern disputes between manufacturers and jurisdiction. As a result, contracts regulate the flow of information to other parts of the regulatory system—including standard-setting, certification, audits, and litigation—and constrain the options that jurisdictions have when their voting systems fail. Gaining a better understanding of how this contracting process has unfolded in the United States will allow us to make recommendations as to how contracts can better support the creation and purchase of trustworthy voting systems. To capture the full diversity of contracts, we have assembled a sample, stratified based on jurisdiction size, of more than 300 contracts spanning the years 1998-2008. Our analysis is ongoing, and we plan to submit our results to a law journal in early 2009. We also plan to discuss our results and recommendations with local and state election officials.

- We submitted a response to the EAC's Request for Information (RFI) concerning a voting system risk assessment. The EAC issued this RFI to collect views about the appropriate scope and objectives of such an assessment. As our comment pointed out, this type of assessment is badly needed to identify hazards to current voting systems. But our comment also counseled caution in the assessment's scope and the EAC's expectations about its application. We argued that, because it is difficult to identify all hazards to a voting system and to quantify the motivations of attackers, it is difficult to fully quantify risk.

Moreover, since threats may be particular to a given voting system, we argued that a single risk assessment framework might not be feasible. We urged the EAC to take these limitations into account when and if it uses the results of the risk assessment to inform security and other standards in the next version of the VVSG (discussed above).

- Joseph Lorenzo Hall filed his PhD dissertation at UC Berkeley's School of Information. Hall's thesis, entitled, "Policy Mechanisms for Increasing Transparency in Electronic Voting", focuses on the issue of transparency in e-voting. After exploring the definition of "electoral transparency", Hall examines the question of e-voting transparency on three fronts. He analyzes the role of disclosed and open source software in election systems and concludes that, while fully disclosed source code is a valid goal, limited disclosure to experts serves many of the same goals in the short-term while preserving vendor trade secrecy. He investigates how contractual provisions between local election jurisdictions and voting system vendors serve to frustrate transparency and finds that election officials need to be more careful in these negotiations. Finally, Hall turns to the question of auditing black box elections systems; that is, since it may be impossible to know how these systems work in the full-disclosure ("white box") case, possibly because of contractual provisions that limit investigation and/or possibly because of proprietary technologies, what methods and procedures are essential for "checking the math" behind our elections.

- David Dill, Eric Lazarus, and Tim King have been developing a comparative evaluation of different voting systems using the "AttackDog" attack tree tool. Our goal is to prioritize security measures for voting, based on the ease of performing various attacks. The premise is that an attack that requires a small number of attackers is more likely to occur and to be successful than an attack that requires a large attack team. Preliminary results show that current controversial measures, such as voter ID requirements that are being imposed in many states, defend against some of the least effective attacks.

Usability and Accessibility

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

- First, Mike Byrne and his students at Rice have conducted follow-up research on the issue of ballot auditability, that is, the ease with which ballots can be hand-counted. This work expands on last year's research in two ways. First, we used a population much more representative of actual poll workers, in particular, we collected a sample with older adults. Second, we examined more ballot types than just thermally-printed VVPATs; this year's work compared VVPATs with optical scan ballots and a video audit trail system based on the Prime III system developed at Auburn University. We found some evidence that the video-based ballots were counted less accurately than the others and clear evidence that the VVPAT ballots were counted more slowly. We also found zero relationship between participants'

level of confidence in the accuracy of their count and the actual accuracy of their count. We are now working on a second follow-up study in which team-based counting procedures are employed.

- Second, we have followed up Everett's dissertation work from last year. In that work, we found that a majority of voters (approximately 63%) failed to notice that the review screen in a DRE failed to accurately display the choices they had made earlier. We generated a new version of VoteBox and the instructions to the voters. This version of VoteBox contained additional review screen information including party affiliation and color-coding of undervotes. The new instructions contained copious reminders for voters to check the review screen. This did increase the incidence of detection, but only to approximately 50%. We suspect this is the outer limit of what can be achieved with simple instructions and visual cues; real change to this rate most likely requires more dramatic changes to voting procedures. We are now working on a follow-up study in which we examine the rate of detection of VVPAT anomalies.

- One concern we have had in our mock election studies of voting is the extent to which the "mock" nature of the election impacts performance. Perhaps people are less motivated to "get it right" in a real election relative to in our laboratory. We examined this by telling participants that their compensation would be a function of how accurately they cast their ballots with more accurate ballots earning more money than inaccurate ones. (We actually compensated all participants as if they had cast perfect ballots.) We were pleased to find that this had no impact whatsoever on error rates, which suggests that the error rates we find in the laboratory are not inflated. We were also concerned that this change would cause participants to slow down in an attempt to be more accurate; in fact, we found the opposite. That is, voters who thought their compensation was contingent on performance actually voted reliably *faster* than who did not. This lends credibility to our previous and subsequent results.

- We have also replicated in several studies a finding we first reported last year, that people strongly prefer the VoteBox DRE to traditional methods such as punch cards and paper ballots, while VoteBox confers no actual performance advantages in terms of objective performance (i.e., time taken to vote, error rate). We reported this as a preliminary finding last year and have now replicated it so extensively that we have no doubt of its veracity.

- We have also added a methodological refinement to our research. Because it is impossible to know the error rates in real elections, various communities rely on "residual vote rate" as a proxy for error. Residual votes include errors such as overvotes, but also include non-erroneous intentional abstentions, and they fail to include errors where the voter casts a vote for the wrong candidate. We have begun comparing the effective residual vote rate with the true error rate, and our data suggest that there are two problems with the residual vote rate. First, it most likely overestimates the actual error rate, and that the residual vote rate is only weakly

correlated with the true error rate. We will continue to examine this further in future studies.

- We have a number of projects in progress this year, which we should be able to report results on next year. First, we have begun working on the issue of accessibility. We are working with a commercial accessibility aid, Vote-PAD, and should be recruiting participants from the Houston chapter of the National Federation of the Blind. We are also initiating work on an auditory version of VoteBox to compare against Vote-PAD. Second, we have completed implementation of VoteBox in Chinese and are collecting data from Chinese-literate voters. This will allow us to replicate earlier findings and extend them to DREs. Third, we have observed in the 2008 election that a substantial fraction of the usability problem reports with election systems involve straight-ticket voting (STV). Straight-ticket voting is an option in 15 states (2 additional states allow it in fairly limited circumstances). However, how STV actually works varies from jurisdiction to jurisdiction and it is clear that even election officials do not always have a clear understanding of how it works in their own jurisdiction. We have developed a survey designed to assess how people think STV works. Based on the results of that survey, we intend to develop alternate implementations of STV on a DRE to assess the impact on usability of different STV schemes.

- We experimented with Gaze-based authentication to reduce shoulder surfing attacks. The system uses infrared sensors to detect the location on the screen where the user is looking. The system displays buttons on the screen and asks the user to look at the buttons in a pre-arranged order to perform authentication. One option is to display a keyboard and ask the user to enter a password using his gaze alone. Our user studies show that the system works well and is easy to use. The net result is improved resistance to shoulder surfing.

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 exit poll analysis and working at the polls. 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.

- Mike Byrne and Dan Wallach co-taught (along with Bob Stein, a political scientist) in Fall 2008 a comprehensive course on elections entitled "Election Systems, Technologies, and Administration." This class looks at voting from a variety of different perspectives. Students in the class are working on two substantial projects. One is an exit-poll analysis, conducted in and around

Houston, which collected data on early voters as well as election-day voters. The second study extended VoteBox to support a VVPAT printer and will conduct human-subject studies to determine the impact of the printer upon accuracy, efficiency, and satisfaction.

- David Dill is teaching a Freshman seminar at Stanford on voting administration and technology issues. Among other assignments, students are required to post weekly on a blog that is shared with Andrew Appel at Princeton University, who is teaching a similar course. Topics include voter registration, voter ID requirements, voting system security, and internet voting. There are several invited speakers ranging from voting rights lawyers to computer scientists involved in voting technology. Students were given credit for working as poll workers, and several did so (along with the teacher). The course web page is (http://chicory.stanford.edu/cs74n/) and the blog is (http://courseblog.cs.princeton.edu/fall08/frs101/). Dan Boneh gave an invited lecture at the course on the importance of open design.

- Avi Rubin covered voting systems for several weeks in a graduate course at Johns Hopkins on Security & Privacy in Computing. The students read several of the recent reports of analysis of voting systems, such as the California Top to Bottom Review, the EVEREST study in Ohio, as well as some of the older reports such as the SERVE study and the Caltech-MIT report. Lectures covered all of the basic voting technologies, their strengths and weaknesses.

Students

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

- Johns Hopkins University:
  - Graduate students: Sujata Doshi, Ryan Gardner, Josh Mason, Matthew Pagano
  - Post Doc: Sujata Garera

- University of Iowa:
  - Graduate students: Robert Hansen, Andrea Mascher, Paul Cotton
  - 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, Cynthia Sturton
  - Undergraduate students: Chris Crutchfield, David Turner, Drew Lewis, Keaton Mowery
  - Clinical Interns: Stephen Dang, Galen Hancock, Cecilia (Peggy) Walsh, Erica Brand, Jason Tokoro, Sarala Nagala

    - Law student: Augustín Núñez, Niki Wood
    - Post Doc/Fellows: Aaron Burstein, , Joseph Lorenzo Hall

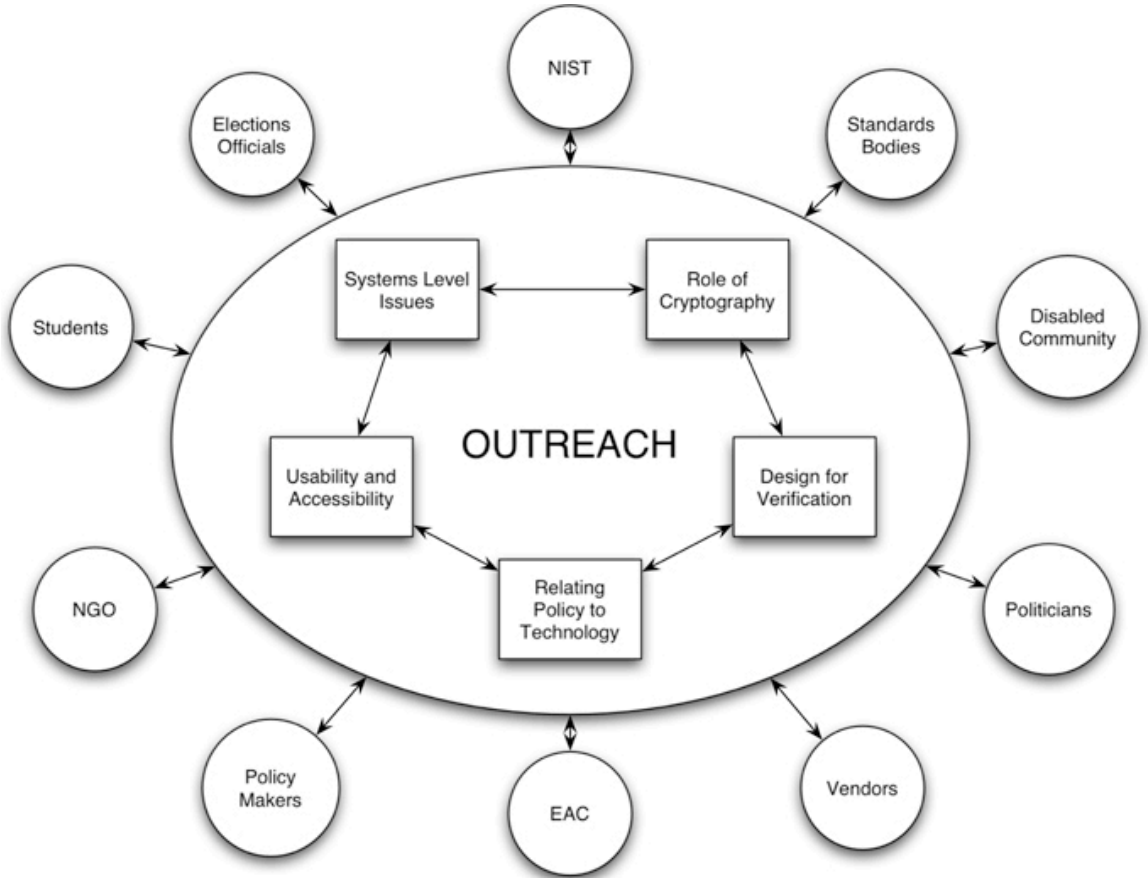
- Stanford University:
    - Graduate students: Eric Smith, Sean Ting
    - Undergraduate students: Tim King

- Rice University:
    - Graduate students: Daniel Sandler, Bryan Smith, Kristen Greene, Bryan Campbell, Jill Piner
    - Undergraduate students: Amy Lin, Stephen Goggin, Emily Fortuna, Kevin Montrose, Daniel Posada, Kathryn Skilton, Kyle Derr (also summer intern at SRI), Corey Shaw, Ted Torous, Adam Purtee

- Other Institutions:
    - John Bethencourt, CMU
    - Tadayoshi Kohno, UCSD
    - Ryan Moriarty, UCLA
    - Josh Kroll, Harvard University

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 2008. 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 2008:

- Joseph Lorenzo Hall spoke on both the West and East Coasts on behalf of the American Bar Association Section on Election Law in order to brief ABA members on voting technology and election policy in preparation for the November general election. Members of the legal and political staff of both presidential campaigns were in the audience.

- The non-partisan Election Protection Coalition – consisting of over 100 non-profit organizations and with over ten thousand volunteers – fielded the OurVoteLive project that allowed voters to call a hotline (1-866-OUR-VOTE) to report a problem, ask a question or request on-site assistance from teams of Mobile Legal Volunteers. Joseph Lorenzo Hall assisted this effort by preparing dossiers on all major forms of polling place voting technologies, fielding novel voting technology incidents in real time on Election Day, and authoring a qualitative analysis of voting equipment reports captured by the OurVoteLive database in the week after Election Day.

- Aaron Burstein and Douglas Jones filed declarations with the Nevada Secretary of State, urging him to rescind an order that severely curtailed election observers' access to polling places during critical pre-election and post-election steps.

- Joseph Lorenzo Hall and Aaron Burstein delivered presentations to the Carter Center's 2008 U.S. Presidential Election Study Mission, which hosted officials and academics from the People's Republic of China as they learned about the U.S. election system and observed the November 2008 general election. Andrea Mascher worked with the Carter Center assisting with a delegation of election observers from China in the United States to observe the 2008 general election.

- Douglas Jones, Andrea Mascher, Aaron Burstein and Joseph Lorenzo Hall are consulting with the District of Columbia City Council and their legal representation concerning irregularities encountered by the DC Board of Elections and Ethics during both the primary and general elections in 2008. This investigation will leverage Burstein and Hall's expertise on voting technologies, post-election audits and voting system contracts and Jones and Mascher's forensic capabilities to develop a framework for sound election technology and policy in the future.

- David Dill co-chaired the EVT 08 conference in San Jose in July. Many election officials participated, including Tom Wilkie, Executive Director of the Election Assistance Commission, California Secretary of State Debra Bowen, Doug Kellner of the New York State Board of Elections, and several local election officials from California Counties.

- David Dill worked as a poll worker in San Mateo county in the November 2008

general election.

- Several ACCURATE members (including Joe Hall, David Wagner, and David Dill) attended a meeting at Berkeley hosted by Karin Mac Donald where we were "walked through" election procedures in Yolo County by election official Tom Stanionis (December 18, 2007).

- Avi Rubin worked as a poll worker in Baltimore County, Maryland in the November, 2008 general election.

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.

- Douglas Jones and Andrea Mascher have been working with the District of Columbia on attempting to understand what when wrong during the canvass of the 2008 DC primary, and in attempting to develop audit centered procedures for avoiding such problems in the future.

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 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.

- Douglas Jones provided oral testimony before the US District Court for Eastern Pennsylvania in NAACP vs Cortes on October 28, 2008 focusing on the likelihood that in any election with hundreds of polling places using any type of electronic voting machines, some polling places will suffer machine failures, and therefore, a prudent election administration will have provisions in place for dealing with failures in advance of the election.

- Douglas Jones testified before a Washington DC Council subcommittee hearing

on election problems in the September 9 primary on October 3, 2008. Jones focused on the need to develop election canvassing procedures that were resilient in the face of failures in the election management system.

- Douglas Jones was quoted at length in "US election: Ghosts in the machine," *Nature 455*, 1171 - 1174 (29 Oct 2008) and in "HAVA Megillah," *National Review 60*, 21 (17 Nov 2008).

- Douglas Jones spoke about voting technology issues on the following occasions:
  - ``The Trials and Tribulations of Electronic Voting," Institute for Civic Discourse and Democracy, Kansas State University, September 16, 2008.
  - ``International Election Observervation," Manhattan/Riley County Kansas League of Women Voters, September 16, 2008.
  - ``International Election Observer -- Kazakhstan and the Netherlands," Iowa City Foreign Relations Council, January 29, 2008. Broadcast on WSUI, 9 PM, February 3, 2008.

- Dan Wallach gave testimony before the Texas House Committee on Elections (June 2008) and the Texas Senate Committee on State Affairs (October 2008).

- David Dill appeared on the Jim Lehrer News Hour, discussing electronic voting security, on January 16, 2008.

- David Dill spoke about voting technology issues on the following occasions:
  - "How America Votes Panel" of Stanford in Government student organization February 28, 2008
  - At the annual meeting of the Marin County Elections Advisory Committee in June 19, 2008 (as featured speaker).
  - A meeting of the interdisciplinary "Liberation Technology" group at Stanford on August 5, 2008 (on electronic voting).
  - INFOSEC Technology Transition Council meeting at SRI in October 6 (as a panel on electronic voting, with Peter Neumann and John Sebes).
  - At a meeting of Stanford alumni on October 10, 2008 (on electronic voting).

- Peter Neumann gave the following ACCURATE-relevant talks:
  - Computer-Related Risks of Untrustworthiness in Life, Liberty, and the Pursuit of Happiness, Lockheed-Martin, March 27, 2008
  - A Short Personal History of Mathematical Beauty in Computer Science, Harvard Computer Society, April 11, 2008
  - Holistic Approaches to Trustworthiness, Security, and Privacy, NSF Cybersecurity Summit 2008 Arlington VA, keynote talk, May 7, 2008.
  - Panelist, Interdisciplinary Workshop on Security and Human Behavior, Cambridge Mass, June 30 - July 1, 2008.
  - Can We Have Trustworthy Elections? Invited speaker for the Women's International League of Peace and Freedom Palo Alto chapter, September 14, 2008.

  - Hour long radio discussion with Jodi Selene, KVMR, Nevada City, California, September 24, 2008, joined in the final fifteen minutes by Gregory Diaz, Nevada County registrar -- who is evidently supportive of ACCURATE's efforts.
  - Integrity of the Election Process, invited lecture, Columbia University, October 6, 2008.
  - Organized and spoke at a session on election integrity, for the quarterly INFOSEC Technology Transition Council meeting that SRI runs for Doug Maughan (Department of Homeland Security Science and Technology Directorate), October 16, 2008. David Dill and John Sebes were the other speakers.
  - Hour-long radio show, Living Room, KPFA, hosted by Kris Welch, with Sascha Abromky, Greg Palast at the beginning, and Zach Roberts at the end, on risks in elections, September 23, 2008.
  - Lecture for the Government Accountability Office staff on integrity in elections, November 20, 2008. (Neumann has been a member of the GAO Executive Council on Information Management and Technology since 1997. The ECIMT meeting the previous day on November 19 included presentation and discussion of the recent GAO reports related to voting.)

- David Wagner was one of three invited speakers to present, in plenary session, at LISA'08: the 22nd Large Installation System Administrators conference. Wagner spoke on the subject of electronic voting.

- David Wagner and Douglas Jones served on a panel ``Electronic Voting, the Politics of Broken Systems,'' at the 2008 RSA Security Conference.

- David Wagner has served as a resource for the press on electronic voting, with quotes appearing in articles and stories published by NPR, ZDNet, Miller-McCune, CNet News, PC World, InfoWorld, SecurityFocus, and others.

- Avi Rubin spoke about electronic voting and the risks of DREs in multiple media outlets including ABC's 20/20, NBC News, CBS News, CNN, NPR, the New York Times, the Washington Post, and the Baltimore Sun.

- Avi Rubin is a co-editor of an IEEE Transactions on Information Forensics and Security: Special Issue on Electronic Voting, starting in November, 2008, with the journal to appear in December, 2009.

- Avi Rubin served as co-editor of IEEE Security & Privacy Magazine's Special Issue on Electronic Voting, 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. 2009 will provide ACCURATE a chance to contribute on many different levels. Our center has already had an impact on the country's elections, and we will continue to work to make future elections as successful as possible and to maximize the lessons we can learn from past elections.

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.

- **Barbara Simons** is retired from IBM Research, where she did algorithmic research in areas such as scheduling theory and compiler optimization. She is a former president of ACM, and the founder of ACM's U.S. Public Policy Committee (USACM). While she has worked on technology policy issues for many years, during the past decade her policy work has focused almost exclusively on voting related issues. She is co-authoring a book on voting technology with Douglas Jones. The first woman to receive the Distinguished Engineering Alumni Award from the College of Engineering of U.C. Berkeley, Simons is also a Fellow of ACM and the American Association for the Advancement of Science. She served on the President's Export Council's Subcommittee on Encryption and on the Information Technology-Sector of the

President's Council on the Year 2000 Conversion. She has testified before both the U.S. and state legislatures and at government sponsored hearings. Simons is currently a member of the United States Election Assistance Commission Board of Advisers.

- **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

Journals

- Joseph Lorenzo Hall, Commentary: Statistical Solutions to Election Mysteries. *Chance*, 2:**21**, 24-25 (2008), *available at:* http://josephhall.org/papers/ash-lamperti_chance-2008.pdf

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*.

- D. Boneh, S. Halevi, M. Hamburg, and R. Ostrovsky, Circular-Secure Encryption from Decision Diffie-Hellman. In proceedings of Crypto 2008, LNCS 5157, pp. 108-125. http://crypto.stanford.edu/~dabo/abstracts/circular.html

- Matthew Finifter, Adrian Mettler, Naveen Sastry, and David Wagner. Verifiable Functional Purity in Java. 15th ACM Conference on Computer and Communication Security (CCS 2008), October 27-31, 2008.

- Mike Byrne, Tiffany Jastrzembski, Douglas W. Jones, Bill Killam, Whitney Quesenbery. Voting Systems Would Benefit from More Attention to Human Factors., Human Factors and Ergonomics Society, Oct. 27, 2008.

- J. Alex Halderman, Eric Rescorla, Hovav Shacham, David Wagner. You Go to Elections with the Voting System You Have: Stop-Gap Mitigations for Deployed Voting Systems. USENIX/ACCURATE Electronic Voting Workshop (EVT 2008), July 28, 2008.

- Joseph Lorenzo Hall, Improving the Security, Transparency and Efficiency of California's 1% Manual Tally Procedures in *The 2008 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'08)* (2008), *available at:* http://josephhall.org/papers/jhall_evt08.pdf

- Arel Cordero, David Wagner. Replayable Voting Machine Audit Logs. USENIX/ACCURATE Electronic Voting Workshop (EVT 2008), July 28, 2008.

- Eric W. Smith and David L. Dill, Automatic Formal Verification of Block Cipher

Implementations, Formal Methods in Computer-Aided Design (FMCAD 08), November 17-20, 2008.

- Peter G. Neumann, Combatting Insider Misuse, with Relevance to Integrity and Accountability in Elections and Other Applications, Dagstuhl Workshop on Insider Threats, 20-25 July 2008. http://www.csl.sri.com/neumann/dagstuhl-neumann.pdf

- Goggin, S. N., Byrne, M. D., Gilbert, J. E., Rogers, G., & McClendon, J. (2008). Comparing the auditability of optical scan, voter verified paper audit trail (VVPAT) and video (VVVAT) ballot systems. In *Proceedings of the 2008 USENIX/ACCURATE Electronic Voting Technology Workshop*.

- Everett, S. P., Greene, K. K., Byrne, M. D., Wallach, D. S., Derr, K., Sandler, D., & Torous, T. (2008). Electronic voting machines versus traditional methods: Improved preference, similar performance. In *Human Factors in Computing Systems: Proceedings of CHI 2008* (pp. 883–892). New York: ACM.

- Ryan Gardner, Sujata Garera, Aviel D. Rubin, Coercion Resistant End-to-end Voting, Financial Cryptography Conference, 2009.

Reports

- Lillie Coney, Juan E. Gilbert, Peter G. Neumann, Erik Nilsson, Jon Pincus, and Bruce Schneier, E-Deceptive Campaign Practices, Electronic Privacy Information Center and The Century Foundation 20 Oct 2008 http://votingintegrity.org/pdf/edeceptive_report.pdf

- Deceptive Practices 2.0: Legal and Policy Responses. Common Cause, The Lawyers Committee for Civil Rights under Law, and the Century Foundation October 20, 2008 http://www.tcf.org/print.asp?type=PR&pubid=149

- Michael Clarkson, Brian Hay, Meador Inge, abhi shelat, David Wagner, Alec Yasinsac. Software Review and Security Analysis of Scytl Remote Voting Software. Report commissioned by the Florida Division of Elections. September 19, 2008.

- Ryan Gardner, Sujata Garera, Aviel D. Rubin, Detecting Code Replacement by Creating a Memory Bottleneck, submitted for publication.

Testimony and Public Comment

- Aaron Burstein and Joseph Lorenzo Hall, *Public Comment on the Voluntary Voting System Guidelines, Version II (First Round)*; Submitted to the Election Assistance Commission on behalf of ACCURATE by the Samuelson Law,

Technology and Public Policy Clinic (2008), *available at:* http://josephhall.org/papers/accurate_vvsg2_comment_final.pdf

- Aaron Burstein, Joseph Lorenzo Hall, Deirdre Mulligan and David Wagner, *Comment on the U.S. Election Assistance Commission's Request for Information Regarding Voting Systems Risk Assessment Support*; Submitted to the Election Assistance Commission by the Samuelson Law, Technology and Public Policy Clinic (2008), *available at:* http://josephhall.org/papers/ucb-eacrficomment-20080428.pdf

PhD Dissertations

- Joseph Lorenzo Hall, *Policy Mechanisms for Increasing Transparency in Electronic Voting*; A dissertation submitted to the Graduate Division of the University of California at Berkeley in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Information Management and Systems (2008), *available at:* http://josephhall.org/papers/jhall-phd.pdf

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.

- D. Boneh, C. Gentry, and M. Hamburg, Space-Efficient Identity Based

Encryption Without Pairings. In proceedings of FOCS 2007, pp. 647-657, 2007 http://crypto.stanford.edu/~dabo/abstracts/bgh.html

- M. Kumar, Tal Garfinkel, D. Boneh, and T. Winograd Reducing Shoulder-surfing by Using Gaze-based Password Entry. In proceedings of the 2007 Symposium On Usable Privacy and Security (SOUPS) http://crypto.stanford.edu/~dabo/abstracts/eyepassword.html

- 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.