

UCVS: Open-Source PC-Based Voting System

Introduction

The goal of UCVS (University of California Voting System)¹ is to enable the administration of public elections in an accurate, affordable, and timely manner, and in a way that inspires voters to have confidence in the election system, satisfying an on-going challenge for democracies for millennia. Successful election administration is an essential feature of a successful democracy.

Modern democracies have developed increasingly sophisticated methods for vote casting, vote tabulation, and for tracking problems with voting fraud. The secret ballot has become enshrined. The voting system needs to ensure that a voter cast one and only one ballot, but, at the same time, there must be no way for election administrators to connect a particular voter with a particular ballot. This requirement for the system to know and, at the same time, not know creates a unique technical problem. Common industrial methods don't apply.

As electronic computers became prevalent in the 1950s and 60s, it has seemed inevitable that they would take on an important role in the administration of elections. After all, they are very good at counting and they are impartial — two characteristics of good election administrators that computers have in abundance. While few would deny their importance, computers bring with them serious problems — both real and perceptual. Some people are overly trustful of them while others fear them. Relatively few people understand them well.

Everyday, millions of Americans use Automated Teller Machines for bank transactions. Customers very rarely have reason to express concern that their \$40 withdrawal might get recorded as \$80 or \$400. We know that we can check our ATM receipts with our bank statements, and they are generally correct. We have come to trust computers to handle our money. Why not trust them just as easily with our vote?

We are not anonymous at the bank. We know what we decided to do and the bank knows it too. They have a record of it and so do we. We can check our ATM receipts against our bank statements and balances. They have several ways to verify any transaction. The trust we have is based on the fact that we can verify the transaction. What if we had no way to know how much the bank really deducted when we withdrew \$40 from the ATM? We would not trust a bank that could not satisfy our need to know that our transaction was handled accurately. If we can't check, we know there will be cheating. The temptation is too great and there is just too much at stake to simply accept a blind claim that everything is being done properly.

Similarly, there is a great deal at stake with our votes, and our trust in the voting system depends on our ability to verify the result. We have accepted the idea that we cannot verify that our individual vote was correctly counted: This is a product of the secret ballot. Instead of verifying our vote the way we verify a bank transaction, we have transferred the verification procedure to election administrators. "Every vote counted" was their motto and the public generally accepted that.

¹ This effort was also called UCVM (University of California Voting Machine).

But election officials have always known that every vote was not always counted. There were always a small but significant percentage of votes that would get thrown out for various reasons. And there were always some voters that should have been able to vote that could not vote, and some ballots that should not be counted that were counted. Prior to Election 2000, documentation of actual performance of voting systems has been poor. Voters from minority groups have been especially prone to disenfranchisement. [Brady2001]

Time-after-time, anomalies in the system were revealed in contested elections. The result of any race won by a sufficiently small margin may be considered technically indeterminate. Such races have been routinely decided in courts depending on who can make the best argument for why a vote should be counted one way or the other. Since there are thousands of times more local elections than national elections, such elections -- where the margin of victory was smaller than the margin of error in the voting system — always happened away from the national spotlight. It was only a matter of time before such an election happened at the national level.

In 2000, it became clear that thousands — perhaps tens of thousands — of voters were disenfranchised in Florida while the difference in the vote count was much less. For the first time in U.S. history, fault after fault in the voting system was revealed on national television. Reaction among election officials was mixed. Some of them said, "I told you so," and some said that the public just didn't understand how elections were really administered.

As a result of the election mess in 2000, repairing the voting system has become a national issue. For the first time, the federal and state governments are providing billions of dollars to modernize the voting system. The voting system is currently in the midst of great change. Within a few years, we will have spent the billions of dollars and we will have a voting system much different from what existed in 2000. But will it be a good system? Will it be better than what we had before? Could it even be worse?

We need to consider some requirements [Brady2003]:

- The secret ballot must be preserved
- Election results must be positively verifiable
- Voters must not be disenfranchised due to registration problems, problems with voting machines, problems related to disabled access, excessive time and trouble, or other technical difficulties.
- The vote count must not be susceptible to manipulation, either by illegitimate ballots being included, or ballot tampering, or by fraudulent tabulation
- The voting system must be affordable

The Help America Vote Act of 2002 (HAVA) purports to address these and many related issues. While the main focus of HAVA amounts to providing billions of dollars that will go to election vendors, it is not clear that the overall objectives will be met or even seriously considered.

- The track record of election vendors in the area of Human Factors testing is very poor.

- Vendors are more interested in protecting their own trade secrets and gaining market share than they are in making their systems open to inspection.
- Lack of transparency means lack of accountability
- Nothing in HAVA will bring voters closer to being able to verify that their vote was counted and counted accurately. They are still simply asked to trust that those charged with that responsibility would do the verification on their behalf.
- Absentee ballot methods currently in use open doors for several forms of hard-to-catch voting fraud. There is little if anything in HAVA to address this problem.
- Absentee ballot methods poorly integrated with poll site methods means that election boards must administer different systems at the same time
- At a time when governments face massive deficits, billions of dollars are being thrown at the problem -- purchasing equipment many times the cost of older technologies. Where will election boards go for the money to replace the new equipment, which will become obsolete quickly?
- The use of Direct Record Electronic (DRE) voting machines is being pushed as a possible solution. They have come under increasing scrutiny because of the difficulty of verifying the purely electronic (paperless) ballot. [Saltman2003]

The Regulatory Context

The U.S. Constitution gives the states the authority to conduct elections. The states in turn give most of the responsibility to the counties. Prior to 1990, there was essentially no Federal role in voting technology, so it was quite proper to characterize the United States as 50 independent states and 4 dependencies when it came to voting systems.

In 1990, the Federal Election Commission (FEC) and the National Association of State Election Directors (NASED) put forth a set of voluntary voting system standards [FEC1990]. These standards were voluntary because the Federal government has no authority to enforce them, but by 2000, a majority of the states had enacted these standards into state law.

Many computer professionals had long been unhappy with these standards, but it was not until the election of 2000 that flaws in these standards received widespread attention [Jones2001a]. This led to an immediate response from the FEC, which released a revised and significantly improved set of voting system standards in 2002 [FEC2002]. It also led to legislative action, in the Help America Vote Act of 2002, taking authority for voting systems from the Federal Election Commission and giving that authority to a newly created Federal Election Assistance Commission, with a strong advisory role being given to the National Institute of Standards and Technology [HAVA2002]. This new standards process has yet to begin serious work.

In addition, several voluntary organizations have begun work on standards applicable to voting systems. OASIS has begun work on standards for data interchange between different components of the voting system, with a goal of encouraging the development of an open-systems model for voting, where various components of the voting system that conform to the OASIS standard could be provided by different and potentially competing vendors.

The Institute of Electrical and Electronic Engineers (IEEE) also launched a standards process, building on the FEC 2002 standard. This process has produced several draft revisions to the FEC 2002 standard, and it has attracted significant criticism. Other players in the evolving standards landscape include the International Association of County Recorders, Election Officials and Treasurers (IACREOT <<http://www.iacreot.com/>>) and The Election Center (<<http://www.electioncenter.org/>>). All of these latter organizations have been criticized for being excessively influenced by vendors and by an interest in preserving the status quo.

Election Technology

The relationship between technological innovation and government management in US elections has been constrained by the economics of designing, producing, and distributing trustworthy voting equipment. Typically, election systems have been designed using technologies that were first adopted—and later discarded—as unacceptable.

The Hollerith card made a hit in speeding up the 1890 census and provided the basis for widespread use of punch card technology in business. When punch cards emerged as technology for data processing in elections, business, aware of the problems of reliability of punch card technology, had already begun to gravitate toward a more reliable scanning technology. More recently, scanning technology has been less popular than touch screen computer systems. For many election administrators and citizens, the emergence of personal computers and networking was attractive because it promised alternative and potentially powerful functionality that could reduce vote-counting error and improve the processing of vote data.

Curiously, the only exception to this rule is the mechanical lever voting machine, developed in the late 1800's and still used today in many voting precincts. In these systems, vote-counting errors are unlikely to be detected unless there is an audit of the election in which the consistency of the internal counters can be scrutinized. Note that when errors are detected in an audit of a lever machine, they *cannot* be corrected.

The evolution of all of these voting technologies has been driven by efforts to minimize costs. Mechanical voting machines, with significant maintenance and moving costs, priced themselves out of the market and have not been produced since the 1930's. The diffusion of newer technologies has been more successful in larger counties and in states such as Oklahoma that adopted a comprehensive, uniform election management strategy and standards.

Historically, technological innovation in election equipment has been limited by lack of uniform, mandatory standards, limited budgets, weak market-demand for better technology, and little incentive for producers to produce higher quality products. Since the 2000 Presidential election, there has been a push for more systematic funding and more rigorous hardware and software standards. HAVA (Help America Vote Act) is funneling \$4.99 billion to “modernize” voting equipment. Companies are paying lip service to building touch screen systems with a paper audit trail for assuring that collected electronic ballots accurately represent voter intent.

Fragmented management of the diffusion of innovative election technology continues to be dominated by short-term considerations, particularly avoiding the embarrassment and costs associated with mismanaged elections. The concern appears to be most focused on providing the *appearance* of trustworthiness and security rather than ensuring *actual* trustworthiness and

security. However, appearance is illusory. People often have an unwarranted confidence in technology, and yet we are all familiar with the concept of a computer error. But most computer errors are in fact people errors, in data entry, system design, or system implementation. Worse yet is the potential for fraud. The rising tide of scandal about DRE (direct recording electronic) voting machines is a result of inadequate testing and validation. The notion of security through obscurity, of keeping mechanisms secret, is inappropriate and potentially an invitation for fraud by insiders. Chiropractors say that the absence of pain is not necessarily health; similarly the absence of scandal is not necessarily correctness.

Although research on the design of voting interfaces is progressing, there has been no effort to develop a set of “user requirements” for the development of new election equipment. What do voters think about the trustworthiness of touch screen systems? Can they recognize breakdowns when they occur? How do disabled voters (e.g., blind) voters feel about what happens to their vote after they touch the screen? Does using a special paper ballot to confirm their votes assure them that the entire voting process is trustworthy?

HAVA repeatedly asks that we investigate how we can best utilize the Internet in our voting system. We also know that election administrators want absentee voting to work as seamlessly as possible with poll site voting. Study after study has rejected the idea of remote unattended Internet voting, but there are other ways to make effective use of the Internet in the conduct of elections. The California Internet Voting Task Force discussed this at length, in their report that came out in the Spring of 2000; they concluded that it was reasonable and feasible to use the Internet at attended polling places, both on election day and in early voting.

Many jurisdictions already allow voters to use the Internet to find their precinct and get a sample ballot. Many jurisdictions already run satellite-polling places in libraries, hospitals and shopping malls during the weeks immediately prior to general elections, typically operating under the law governing absentee balloting. While they are conducted under absentee rules, the operation of these satellite polling places overcomes most of the widely understood problems with pervasive postal voting – voters at a satellite polling place cannot disclose their ballots, allowing payoffs for correct voting, and the ballots are not subject to postal mishandling.

Therefore, we propose to investigate appropriate use of the internet both for collecting ballots from regular polling places and from satellite polling places. With appropriate changes to state law, this could, potentially, allow absentee voters to vote from any satellite polling place or county courthouse without the need to plan in advance for an absentee ballot request. National adoption of appropriate standards could allow such absentee voting across state lines.

From an economic perspective, innovation in election technology can be provided using market and non-market mechanisms for producing and distributing better voting systems. Although weak consumer demand and the lack of uniform standards have limited the efficiency of market-based production and distribution of machines, the market has provided a means of overcoming the problem of “free riding” that can occur in non-market production and distribution processes. In such processes, voluntary production of better technology will not work if the costs of production are not covered by revenues or the financial and/or personal labor contributions of leaders who value the public good enough to create it for everyone else. [Olson1965] [Mueller1989]

There is a nascent movement of public-spirited developers who aim to provide a referent, public domain set of software voting tools that meet the highest possible standards of usability, security, and management accountability. This movement, structured around an Open Voting Consortium, would use a community licensing strategy to produce and distribute a public good: free election software. Under a community license, all source code is made available for non-commercial, experimental use. Developers agree to contribute any new code back to the community, which integrates this work into official releases that have passed tests according to standards set by the Open Voting Consortium.

Proposed Approach

Our project will include a combination of research and development/demonstration.

Our research efforts will include:

1. Analyzing current rules and regulations as well as standards on voting systems and creating a taxonomy of approaches.
2. Designing a model standard for verification in ballot management.
3. Producing a baseline analysis of the implications of verifying ballots for blind voters.
4. Proposing a framework of options for managing election software to ensure privacy protection, to deliver trustworthy voting services, and to resolve conflicts over the implementation of different voting methods.

We will also develop a PC-based open-source reference system for a voting machine with a voter-verifiable ballot. This reference system will be designed for validation and extensibility. Our objective in developing this reference system is two-fold. First, the reference system will illustrate and demonstrate the concepts we are studying. Second, the reference system can form the basis for other organizations to develop complete production voting systems including tabulation and reporting.

Related Work

The recent risk assessment for the Diebold AccuVote system commissioned by the State of Maryland [SAIC] clearly illustrates that current election practice, current voting systems, and indeed, the current system of voting system standards and certification put in place by the National Association of State Election Directors and the Federal Election Commission [FEC2002] are deeply flawed.

We view the security and integrity of the voting system as being central to the national security of any democracy. Therefore, it seems prudent to evaluate voting system security using the same terms we use for national security. Several of the requirements for voting systems are quite different from those used in conventional secure computing, but the overall defense in depth [IASG2003] strategy used for the construction of secure systems is certainly applicable.

Several vendors and researchers have proposed models for the conduct of voter verifiable elections; for example, Rebecca Mercuri's model [Mercuri2002], with a paper record displayed to the voter behind glass [Mercuri2002], and the Populex digital paper ballot [Populex], where the voter carries a machine generated paper ballot from the voting machine to the ballot box.

Hand-marked ballots read by optical mark-sense scanners also provide for voter verifiability, and there have been cryptographic proposals for voter verification for many years [Chaum1981].

While there have been initial stabs at organizing a taxonomy of voting systems, for example, by David Chaum [Chaum2001], the variety of voter verifiable systems has not been dealt with, and the question of whom you must trust to run a verifiable election has not been extended to deal practically with the actual methodology for conducting an audit of an election. Each of the voter verifiable audit trail models is subject to different threats and a useful taxonomy must be based on threat assessments for these models, along with procedural recommendations for the use of voting systems following these models.

Caltech/MIT

In the wake of the election mess in 2000, the presidents of Caltech and MIT directed the launching of a project they hoped would bring about a solution to the voting system problem. Their 14 December 2000 press release [Caltech2000] began:

The presidents of MIT and Caltech have announced a collaborative project to develop an easy-to-use, reliable, affordable and secure United States voting machine that will prevent a recurrence of the problems that threatened the 2000 presidential election....

“It is embarrassing to America when technology fails and puts democracy to such a test as it did this month,” said Caltech President David Baltimore, who opened the hour-long live teleconference in Pasadena, California.

“Academic institutions have a responsibility to help repair the voting process so that we don't see anything like this again. This project is intended to protect the system from the problems we've seen in the last election,” Dr. Baltimore said....

“We must find a solution. Each of us must be confident that his or her vote has been reliably recorded and counted. A country that has put a man on the moon and an ATM machine on every corner has no excuse,” said Dr. Vest.

In their project update of January 2003 [Caltech2003], they state that in the summer of 2001 they published “Voting: What Is, What Could Be,” their “first major report on the problems in the electoral process.” The immediate recommendations were:

- Replace all punch card and lever voting machines with new voting systems
- Improve voter registration systems, in particular, implement the aggressive use of provisional balloting

They mentioned that they have won a contract with the DoD to develop an Internet-based absentee voting system for military personnel overseas.

They also announced the development of an architecture “that would allow election administrators to use school computers as voting machines.” Dual use of commodity PCs for use as voting machines is a concept included in the 2001 Brady-Dechert proposal for California [JHUonVCB] [Brady2001a]

Caltech/MIT does not see market failure as a problem; we see it as a problem to be assessed and addressed with an open source approach. Also their study does not focus on end-to-end security; we aspire to do that. Unlike the UCVS, the Caltech/MIT project shows no commitment to the open source model or the voter-verified printed ballot.

More recently, the Caltech/MIT project has published their report on "Voting in Massachusetts," [MA2003]. This report recommends Election Day Registration (ERD), and generally encourages Massachusetts to embrace concepts that are promoted in HAVA. They also encourage election boards "to lease, not buy, new voting equipment."

Univ. of Maryland

Researchers at the University of Maryland are conducting human factors and economic studies of a zoom interface to improve active verification of votes, but do not aim at multiple levels of verification (including the server level) that will be explored in our proposed research. In addition, these researchers are investigating the implications of the use of alternative voting methods, but our project will focus on problems of passive and active auditing of voting with different voting methods for end-to-end security, particularly for blind voters. Finally, although the Maryland researchers are concerned with better election management, they are not assessing broad options for changing the economics of technological innovation in the development of election systems.

eVACS®

In October 2001, the Australian Capital Territory (ACT) adopted eVACS® electronic voting machines in a limited number of polling places, as well as electronic tabulation of electronically recorded and scanned ballots. [ElectACT] With the success of the initial effort, it is anticipated that eVACS will be extended throughout the ACT, and to the rest of Australia, over several election cycles. eVACS was developed by the Australian company Software Improvements, and underwent independent audit and testing.

eVACS is a GPL Free Software system, and operates on commodity PCs using a minimal version of the Debian Linux operating system. Accommodation is provided for blind, visually-impaired and mobility-disabled users, and operating instructions and ballots are available in multiple languages. eVACS, however, is a DRE system, with vote selections stored only on a locally networked server (with no external network connection). eVACS also implements tabulation according to the ACT's complex Hare-Clark electoral system (a variant of Instant Runoff Voting), which is not used in any USA elections. On the other hand, general elections in the United States are more complex than the elections in other countries because of the number of races involved.

The human interface to eVACS consists of a horizontally mounted 17" display on which a ballot is displayed, and an 8-button keypad to navigate contests and selections. Disabled voters may use a special voting station that contains a 21" vertically mounted, screen, allows wheelchair access, and contains headphones over which voting instructions and selections are read as each button is pressed. Buttons also have tactile labels. As each navigation press is made, the instructions read over the headphones explain the current status, contest, and selection. Even if utilizing the optional vocal instructions, a disabled voter will press the same key sequence to complete a ballot as any other voter.

EVM2003

EVM2003 is an open-source project actually underway, and hosted by SourceForge. This project is being led by Dr. David Mertz, Dr. Arthur Keller, and Alan Dechert, all of who are participating in the effort in this proposal, and includes an international team of volunteer developers. This project is producing a limited-purpose demonstration of the general concepts. EVM2003 is intended as a (1) demonstration system, (2) testbed for concepts destined for UCVS, and (3) as the potential basis for future projects other than UCVS, such as a non-USA or non-governmental voting project.

OVC (Open Voting Consortium)

OVC is a non-profit trade organization in formation and founded by Alan Dechert. The goal of OVC is to establish guidelines and standards of practices for software developers, service providers, and election officials in the use of open-source voting machines with a voter verifiable ballot. The objective is for the OVC to be a path of technology transfer for the software developed by this proposal.

Research Questions and Strategies

The project will investigate the following questions about a public goods model for developing and delivering free election software. For each question, research strategies and issues are described.

Question 1: How can software be developed to resolve the paradoxical relationship between anonymity and privacy?

Absolute anonymity is often associated with absolute privacy, but paradoxically, end-to-end security in voting requires being able to identify some or all attributes of a voter to actively verify votes. This requirement is necessary to assure that:

- A vote is cast that correctly represents the voter's intent,
- The vote is correctly recorded in the database, and
- The vote is counted correctly when all votes are aggregated.

Collection of votes in local networks and/or wide area networks poses challenges for developing mission-critical standards and state-of-the-art software tools. How can new techniques for trustworthy software be employed within an Open Voting Consortium framework? These techniques include:

- Program analysis: profiles for running programs to prevent malicious and/or unintentional errors associated with memory access, storage, and use of system/network resources. [Sabelfeld2003] [Schneider2000]
- Model checking: detection of abnormal transactions in collecting and processing votes, and
- Type-safety: runtime proof that software does not contain problematic code. [Compagnoni2003]

How close are these techniques to being translated into protocols and languages that can be integrated into public domain knowledge? What skill sets and training are required to make use of these techniques? Would implementation of these standards increase or decrease the cost of managing an election?

This question will be addressed in interviews with technical specialists. A literature review will also be conducted to survey opinions about developments in these areas.

Question 2: What new issues will be raised by enabling the implementation of alternative scoring methods?

National organizational advocates of alternative voting methods have been campaigning to assure that election software enables rules such as Approval Voting (casting one vote for each approved choice) and IRV (Instant Runoff Voting) (using ranked preferences to resolve tied and close election outcomes). Ideally, election software should be neutral so that whatever users want can be implemented. But the software must be developed to be able to handle the systemic requirements of alternative voting methods. These requirements include

- Reports for individual citizens, election officials, and media
- Plan for detection and resolution of voting paradoxes
- Plan for detection and resolution of ties

Ties are more probable under certain methods than others. For example, ties are more likely to occur under constrained approval voting (m of n candidates approved where $m < n$) and unconstrained approval voting (m of n candidates where $m \leq n$)

Moreover, IRV is often implemented with different assumptions about how voters can rank choices (e.g., in some elections, voters cannot rank more than one candidate for a particular rank) and how votes should be processed to resolve collective outcomes (such as ties or close outcomes) in which a single choice must be identified. Some practitioners produce a single winner by deleting the candidate with the most last place votes, while other users delete the candidate with the fewest first-place votes.

Alternative methods also have implications for the usability of software interfaces as well as procedures for auditing the election process from the precinct to the final depository of votes. What are these issues and how can they be addressed?

Question 3: How would community licensing affect the management of elections?

Can a set of “user requirements” for elections be developed for orienting the work of an Open Voting Consortium? Would innovation be driven by more citizen input, particularly from members of the community knowledgeable about computer systems and software? Independent Testing Laboratories would not be needed, but political parties might hire them or their own consultants to scrutinize the work of the Consortium. Would there be bipartisan support for a more highly trained professional class of election managers? Or would large and small consulting companies be retained by states and/or parties to evaluate licensed code? Would software depositories still have a role to play in the management process or would their function become unnecessary?

Under what social and technological conditions would opt-in citizen participation enable governments to become infomediaries to pay for the infrastructure and management costs of electronic elections? What types of information could be linked to election data and which industries would have an incentive to bid on access to citizen information? Would the information have to include an individual's actual vote or could the voting data be linked to data derived from episodic or periodic opt-in responses to questions about marketing issues? What affects would such arrangements have on marketing, political polling, and Web panel research? What would be the impact of a government information broker be on marketing, political polling, and Web panel services?

Question 4: How should software be designed and implemented to facilitate validation and verification?

Typically, software is implemented and then it is tested. Often components are implemented and tested separately and then integrated and tested as a whole. But software testing can demonstrate only the presence of bugs, not their absence. Certainly open source software has the advantage than anyone may inspect it and look for bugs, trapdoors, and errors in logic or implementation.

Proving a program correct is impractical, and even at that merely ensures that the program meets the specifications, which themselves may be faulty. [Rapide] How will using self-checking techniques akin to defensive programming or paranoid programming reduce both the chances for error and for fraud? [Cheswick2003] Is it effective to create errors or trapdoors deliberately during development to challenge the testers and community to find them? What should a voting system do in a production environment if it detects an error? Is there a benefit to automatic crosschecks to detect errors or attempts at fraud? Are there situations in which an automatic crosscheck will detect a problem that cannot be corrected? Or can we preclude such situations through appropriate design?

Question 5: How do the different proposals for voter-verifiable ballots relate to each other?

We hypothesize that there are broad classes of voter-verifiable election machinery that share common threats and depend on similar administrative controls to address those threats. To date, there is no effective classification of models of voter verification or election auditing, and we propose to develop one, working through the threats and appropriate administrative controls for each class we identify.

One of us (Jones) has produced threat assessments that analyze the defenses applicable to voting systems [Jones2002a] [Jones-a] [Jones-b], and we propose to expand on that work to cover the different approaches to voter verified ballots as well as to security assessments that have been done of direct recording electronic voting systems [SAIC].

There are a variety of standards and regulations that apply to elections, coming from multiple overlapping jurisdictions and organizations. Understanding the complex interplay of these standards and regulations and detecting conflicts and inconsistencies (and holes!) is a problem in other regulatory frameworks as well. [Regnet]

We believe that this part of the project will have significant broad value, and we believe that the value of this part of the project will be enhanced by the use of a specific example, the UCVS reference system, as both a test case and an illustration. Such an example should have significant value to voting machine vendors and to state and local election administrators interested in evaluating the security of their voting systems in their local administrative context.

Question 6: Can Remote Attended Internet Voting and Mobile PC Voting Machines replace current absentee ballot systems?

Mobile voting stations have been deployed in the State of Oregon as a way to reach house-bound voters. The proposed UCVS system would have all the ballot data for a county on one CD so that ballots for individual precincts can be produced on-the-spot by entering the precinct number. The voter using the mobile system could see the same screens as the poll site voter for a given precinct. The printed ballot could also look the same as poll site systems (ballot mailed on the spot instead of dropping into the ballot box). Similarly, a remote Internet voter at an attended station could see the same ballot on-screen as poll site voters and print in a similar manner. In these modes, both the electronic record of the vote and the printed ballot could look the same as poll site electronic and paper ballot images.

Included in this work is the use of interviews with researchers at Caltech/MIT and the University of Maryland, as well as election officials knowledgeable about election management as well as blind voters. These interviews will be followed up with annual Web surveys directed at an expert panel of developers, academics, and election officials and interviews with blind voters, and leaders of support groups for the blind.

A human subjects protocol for conducting these interviews and surveys has been filed with the Stevens IRB. Copies of the proposed privacy and procedural documents are linked to this proposal under Supplementary Documents.

Project Management

A variety of expertise will be brought to bear on this project through a consortium of three institutions and several consultants. Overall project management will be done by the University of California at Santa Cruz (UCSC). Researchers from the University of Iowa and Stevens Institute of Technology will play important roles in this effort.

Overall scientific management will be done by Prof. Pat Mantey of UCSC. Prof. Mantey also serves as UCSC's lead on University of California's CITRIS (Center for Information Technology Research in the Interest of Society).

Day-to-day project management will be done by Dr. Arthur Keller of UCSC. Dr. Keller managed several research projects while at Stanford University, including the development of the Infomaster system for integrating heterogeneous electronic catalogs. Infomaster was licensed to Mergent Systems, which Dr. Keller co-founded and was acquired by Commerce One in January 2000. Dr. Keller was also Chief Technical Advisor and board member of Persistence Software, which went public in June 1999. Dr. Keller will also serve as Chief Programmer on the project, leading a team of students at UCSC in the development of software for this project.

Prof. Doug Jones of the University of Iowa will lead the effort to analyze current rules and regulations and voting system standards to develop a taxonomy of audit models for voting systems. His experience with voting system standards [Jones2001a, Jones2002a, Jones2002c] and his experience with state election procedures puts him in a unique position in this field.

Prof. Arnold Urken of Stevens Institute of Technology is a political scientist who will lead the effort to design a framework of options for managing election software to ensure privacy protection, to deliver trustworthy voting services, and to resolve conflicts over the implementation of different voting methods. Prof. Urken will also manage the team of external consultants providing assistance to this project. These consultants include:

Alan Dechert, who has devoted the last 3 years of his life to the development of an PC-based open-source voting machine with a voter-verifiable ballot. Mr. Dechert will be the liaison to people external to the project, such as standards bodies, elections officials, elected officials and their staff, used-PC remarketers, to track their activities and to foster an environment where the results of our efforts will have an impact.

Dr. David Mertz is currently leading the effort to develop a PC-based open-source demonstration voting machine with a voter-verifiable ballot, called EVM2003. This project, involving about a dozen volunteers from around the world, started in July 2003 and will be shown in a public demonstration of our concepts before the end of 2003. We will expand this effort to have components of our software developed in this distributed volunteer manner. Dr. Mertz will coordinate the external contributory effort.

Prof. Peter Maggs of the University of Illinois at Urbana-Champaign is a professor of law. Prof. Maggs is an expert on Internet and computer law. He also did pioneering work on computer applications for blind and speech-handicapped users. He will provide valuable input in the legal and technical issues of supporting voters who are visually impaired. He will work with Prof. Urken to produce a baseline analysis of the implications of verifying ballots for blind voters

Technology Transfer Plan

To facilitate the adoption of the technology we create, we are releasing the software produced under the proposed effort under the EVMPL (Electronic Voting Machine Public License), which is an extension of GPL (Gnu Public License) that requires the edit history to be maintained. We will work closely with the Open Voting Consortium to provide assistance in extended and completing the system, achieving certification for the software and system, and in development of standard practices for elections officials, and for elections equipment vendors and service providers using open-source software based on our results. The use of volunteers for the open source community in voting technology has been proven successful in the EVM2003 project (hosted by SourceForge), led by several of the people on this project. Furthermore, these volunteers will provide continuity during the transition to the Open Voting Consortium.

Statement of Work

UC Santa Cruz – Mantey and Keller

Year 1 – During the first year, we plan to survey and determine the applicability of self-checking defensive programming or paranoid programming techniques for the development of the

voting system. We will also develop the computer system architectures and encompassing processes and procedures for the voting system.

Year 2 – During the second year, we plan to develop the first generation working prototype voting machine for testing, validation, and experimentation.

Year 3 – During the third year, based on the results of the other groups, we will develop a complete working voting machine and ballot reader for the visually impaired and working prototypes of tabulation and reporting components of the architecture.

University of Iowa – Jones

Year 1 – During the first year, a literature survey will be undertaken, directed by the needs of building a general framework for the evaluation of voting systems both technically and in their administrative context.

Year 2 – During the second year, we plan to build a general taxonomy for voter verifiable voting systems and construct threat models and suggest technical and administrative countermeasures for each threat in terms of each taxonomical category.

Year 3 – During the third year, we plan to apply our methodology to the UCVS, evaluating this system against the threat models and working out a recommended model set of administrative procedures for use with this system.

Ongoing – In addition, during all three years, the Iowa group will continue Doug Jones' ongoing efforts to track, criticize and contribute to the evolving voting-system standards.

Stevens Institute of Technology – Urken

Year 1 – During the first year, the research assistant and the PI will review the state-of-the-art in voting security and interfaces for blind voters, working with Dr. Maggs to develop and implement some pilot talk-through experiments with sighted and blind students involving ballot verification and the understanding of alternative voting method rules. We also plan to form a Web panel of expert respondents on the economics of technology transfer associated with the concept of the government as an information broker.

Year 2 – During the second year, we plan to expand our experiments and surveys and produce a model standard for blind interfaces and information brokering.

Year 3 – During the third year, we plan to incorporate our experimental findings in the UCVS software and evaluate its operation from technological, economic, and user viewpoints. We also plan to present a model of the role of government as an information broker for public comment.

Results of Prior NSF Support

Arnold Urken – Stevens Institute of Technology

NSF Project CCR-0220286, \$292,000, 09/03-05/04, Secure Electronic Transactions

An analysis of Roberts Rules of Order as a natural system that incorporates logic tools for communicating votes with end-to-end security. Roberts Rules of Order can be seen as a system that incorporates informal methods for actively verifying the casting and counting of votes. These standards can be considered for electronic transactions. Banking transactions come closer than voting transactions to achieving this goal.

Arnold Urken, “What We Can Learn from Roberts Rules of Order About Voting Security” (pending, Communications of the ACM). Longer version in draft form being circulated for comment.

No available data, samples, physical collections and other related research products not described elsewhere.