

## Prime III: One Machine, One Vote for Everyone

E. Vincent Cross, II<sup>1</sup>, Gregory Rogers<sup>1</sup>, Jerome McClendon<sup>1</sup>, Winfred Mitchell<sup>1</sup>, Ken Rouse<sup>1</sup>, Priyanka Gupta<sup>1</sup>, Philicity Williams<sup>1</sup>,  
Idongesit Mkpong-Ruffin<sup>1</sup>,  
Yolanda McMillian<sup>1</sup>, Elizabeth Neely<sup>1</sup>, Jamare Lane<sup>1</sup>, Harold Blunt<sup>1</sup>, Juan E. Gilbert<sup>1</sup>

<sup>1</sup>Department of Computer Science and Software Engineering  
Human Centered Computing Lab  
Auburn University  
107 Dunstan Hall  
Auburn, AL 36849

{crossev, rogergd, mccleje, mitchw4, rouseka, guptapr, willipk, mkponio, mcmilym, neelyea, lanejam}@auburn.edu,  
harold.blunt@asurams.edu, gilbert@auburn.edu

### **Abstract**

Has voting technology ever allowed all segments of the voting population to vote privately, securely and independently with equal access? In short the answer is no. In an effort to address this very issue a usable and secure (usable security), multimodal electronic voting system that allows voters to vote using voice, touch or both was developed, Prime III. Prime III is one machine that gives equal access to the electoral process for all citizens.

### **Electronic Voting Issues**

#### *Mark-sense ballots*

Mark-sense ballots also known as, optically scanned paper ballots, list the candidates' name or issue next to an oval, square, or circle. The voter marks his or her choice by filling in the oval, square or circle. Once done, they can take their ballot to a scanner which records their vote by using "dark mark logic" which recognizes the darkest mark for a given set (Optical Scan Voting Systems, 2007). This form of voting has a low learning curve and is easy to implement. However, issues do arise when the scanner can

not recognize the darkest mark so there is no way to guarantee that your vote will be recorded properly. This issue also lends itself to subjectivity in recounts, e.g. determining the voter's intent based on unclear marks. There is also the issue of maintaining the millions of mark-sense paper ballots. In addition, mark-sense paper ballots are not user friendly towards disabled or illiterate voters. Additional special accommodations have to be made for voters with various disabilities.

### *Direct Recording Electronics (DRE's)*

DRE's such as touch screens are the latest systems in electronic voting technology. Developed in the 20th century, these systems use touch screens that list the names of the candidates and issues. The voter votes by touching the name or issue on the screen that s/he wishes to cast a vote for. In most DRE systems, there is no physical ballot; the votes are tabulated by the system itself. The tabulated votes are stored in either a local database or if networked in an offsite database. There are a number of risks associated with DRE; vulnerability to hackers, malignant workers, faulty code, lack of recount ability, and human error {(Feldman, 2006), (Hursti, 2006), and (Kohno, 2004)} **Error! Reference source not found.** DRE once hailed as the future of voting, have come under intense scrutiny due to these inherent risks.

The majority of the security and usability concerns are not limited to a few manufacturers. On the contrary, all of the manufactures of DRE machines have experienced a number of security issues. Very few, if any, of the manufacturers have allowed voluntary outside review of their code, which has caused even more alarm as noted in a HBO documentary "Hacking Democracy" (HBO, 2006). Faulty code in an election can cause votes to be lost, and/or allocated to the wrong candidate. A larger concern is code that has been introduced by a programmer solely for the purpose of throwing an election. Such functions could be hard to discover even during formal inspections. In addition, there are other concerns such as smart cards used in some precincts can be faked, that hackers could gain access to the system via internet and corrupt the election, and databases which stores the votes could be manipulated. All of these security issues have been raised by numerous security experts all over the nation and trumpeted by the media. Finally, according to the Help American Vote Act (HAVA), all Americans should have equal opportunity to cast their votes (107<sup>th</sup> Congress, 2002). This requires that each precinct have at least one machine that is usable for disabled voters. Optical scan and DRE systems provide various techniques to allow seeing impaired voters the ability to vote however, current optical scan and DRE systems fall short in being usable by voters who are illiterate, have a physical disability or any other disability that prevents

them from using a touch screen or pen and paper. Due to the number of issues and lack of solutions, an alternative approach that meets HAVA requirements and is founded in research and user centered design principles (Robertson, 2004) has been developed called Prime III.

### Prime III

Prime III is a secure, open-source, multimodal electronic voting system that delivers the necessary system security, integrity and user satisfaction safeguards in a user friendly interface that accommodates all people regardless of ability. Essentially, if you are illiterate, can not see, hear or if you have a physical disability, i.e. arthritis, you are still able to vote using Prime III in a private, secure environment without assistance.

Prime III is incorporated into the current voting process that the voter is accustomed to using. The voting process begins when the voter enters the voting precinct and is verified using the standard procedures in each precinct/state. When the voter enters the voting area, s/he will be assigned a voting booth by a poll worker.

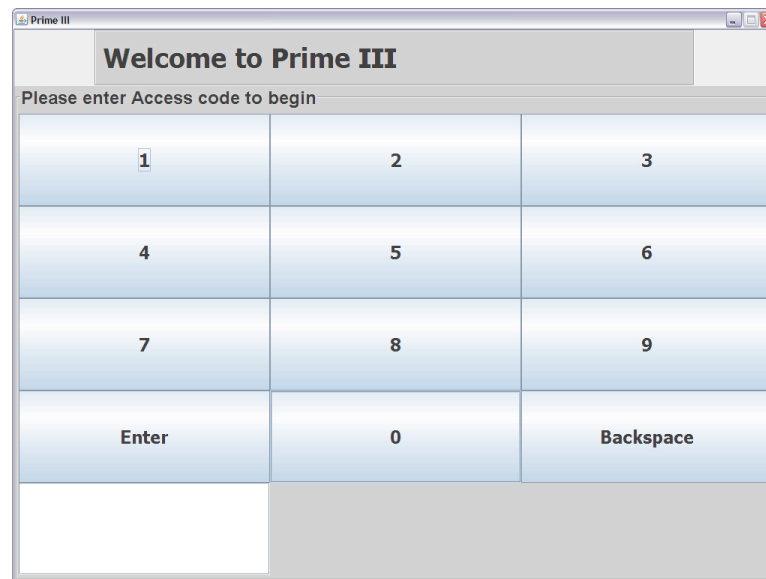


Figure 1: Poll worker authentication screen

When the booth is available, the poll worker will load the ballot using her/his poll worker ID, figure 1, replace the headset sanitary covers and the voter will enter the booth.

If the voter needs assistance entering the booth, the poll worker or necessary individual(s) can help the voter. Inside the voting booth, the voter will use the touch screen or the headset, to cast her/his votes. Note that the voter can choose to use either the touch screen and/or the voice enabled headset at any point during the election process. For voters using the touch screen, Prime III uses large fonts with neutral colors for people that are color blind figure 2.



Figure 2: Sample Prime III screen with voice prompts and possible user responses

Note that each office lists the candidates in a single column. This ballot design removes ambiguity and confusion by only showing the candidates for one office at a time where other systems show multiple offices per screen, which is simply copying the paper ballot to the screen. Paper to screen voting systems are bad design.

Voters that use the headset to vote will receive prompts that speak the ballot options currently displayed. Each option is randomly assigned a number. If the choices are Democrat, Republican, Green Party; Prime III will prompt the user with something similar to "Say four to vote for the democratic party <beep> say three to vote for the republican party <beep> say two to vote for the green party <beep>". The voter will simply speak the number associated with her/his choice. As such, eavesdroppers will hear a voter speaking numbers with no indication of the voter's choices. For example, assume two voters, Arthur and Irma, enter separate voting booths. If you were to eavesdrop on these two voters, you may hear Arthur saying "five, seven, three, eight" and Irma saying "two, five, one, nine". In this scenario, Arthur and Irma could be voting for the same officials, however, no one would know by simply eavesdropping on their conversations with the machines. Note that this is different from other voting systems by which the voter either hears the options and then uses Braille coded buttons to make their intent known or the voter uses a human proxy to record the voter's votes. To our knowledge, Prime III is *the* only voting system to take full advantage of a speech interface by using automatic speech recognition. During voting, the voter will be required to confirm her/his ballot twice. After the second confirmation, the voter's ballot will be stored to the hard drive and the ballot application will close. At the same time, the voter's entire session was recorded through the use of a video recorder directly connected to each Prime III. The video recorder monitors each Prime III machine. There are no video cameras used in the implementation. Note that neither the voter nor the voter's voice is recorded on video only the screen and Prime III's audio. The voters' identity remains anonymous. The video recorder facilitates a unique method of recount. After casting their ballot, the voters will exit the voting place.

### *The Prime III Security Model*

The Prime III open environment facilitates security. The entire process is open to the public and highly visible. In figure 3 you will notice that there is a separation between the user and the Prime III system. The Prime III system is not physically located in the voting booth; it is in a separate partitioned area under guard. The user interacts with the Prime III system as previously mentioned either through the touch screen and/or the headset. By removing the system from the voting booth it prevents a voter from tampering with the system during the election. In addition, this limits the interaction abilities of the user by limiting access to only touch and headset. No one is allowed to touch the actual voting machines nor is anyone left alone with the machines during the election. The Prime III open environment is also designed to allow voters to view the machines, poll workers/guards, and each other, but not each others screens. The only hidden aspects of the system are the actual touch screens and headsets as illustrated in figure 3.

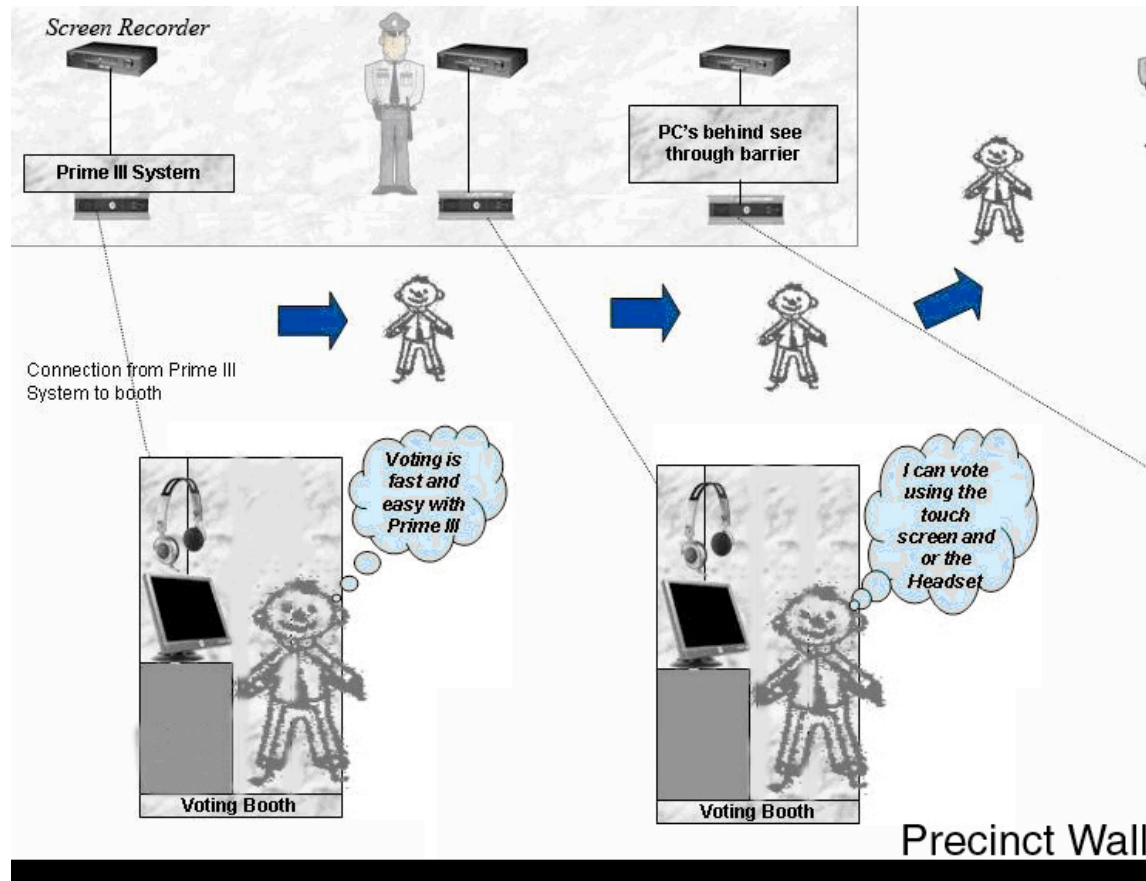


Figure 3: Prime III voting environment

Prime III incorporates a number of software security measures in addition to the open environment physical security. Prime III can run on either Windows or SELinux (Security Enhanced Linux, 2006), operating system. Prime III will use the authentication on Windows or SELinux to restrict user access to each machine. On top of the restricted user access, Prime III uses a combination of imposter files and encryption to secure the election. Imposter files are vote files located randomly through out the system. The imposter file concept is illustrated in figure 4.

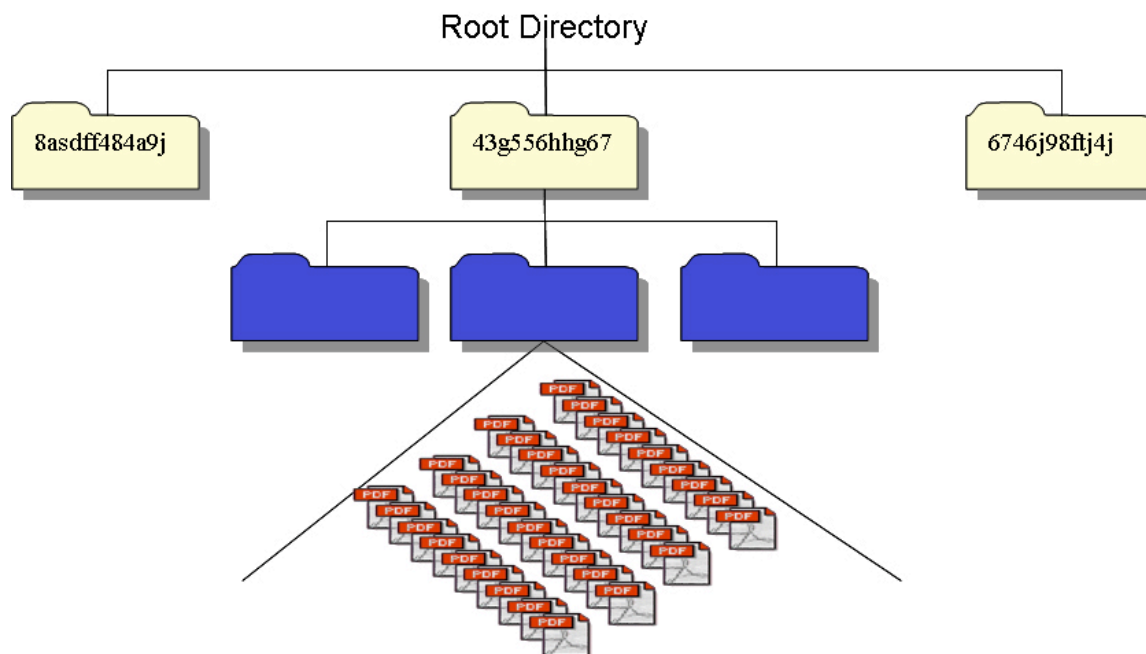


Figure 4: Imposter File Organization on Prime III

Under the root directory, there are several imposter folders, each with different names and no identifiable patterns in the names. Each folder contains 500 subfolders. Each subfolder contains encrypted portable document format (PDF) images of voter ballots. These ballots only contain the voter's selections. Each ballot contains a date time stamp of when the ballot was cast. The encrypted PDF ballot files are assigned to one of the 500 subfolders at the time the ballot is recorded. At the same time, several other randomly generated encrypted PDF ballots are written at random to other imposter folders. There is only one real vote folder and that folder is determined by an input key set by the election administration official. Each file, whether real or an imposter, is encrypted with Triple Data Encryption Standard (Triple-DES), Advanced Encryption Standard (AES) or other encryption algorithms. The encryption method used for the imposter files are pre-assigned and may vary from precinct to precinct. This approach makes finding the actual vote on the system extremely difficult, essentially, this security approach makes finding a needle in a haystack seem plausible as this is more like finding a specific strand of hay in one of many haystacks. If

a hacker was to gain control of the Prime III machines, he would still have to overcome the video surveillance.

Prime III uses video as an added security and auditing measure in the form of video surveillance of each machine. A separate video recorder is attached to each Prime III machine figure 3. The video recorders record all on screen interactions with an on screen date and time stamp. They do not record the actual individuals voting, therefore, the voters' privacy is not compromised. In the event of an attack on Prime III voting machines, the hacker would have to overcome the restricted user access measures on Windows or SELinux, break down the encryption schemes of the encrypted PDF ballot files, determine the correct ballot file and circumvent the video feed, such that it can't be noticed. Ultimately, this provides a reproducible trail of what actually occurred on each machine for security, audit and recount purposes.

During an audit or recount the voters' intent will be clearly captured on each video recorder via the recorded screen and the recorded audio from the Prime III system. Election administrators will be able to watch the election and tally the votes of the voters as they actually occurred. The video surveillance is an improvement to the Voter-Verifiable Paper Audit Trail (VVPAT) (Shamos, 2007).

### **Future Work**

Prime III will undergo an extensive security scrutiny from security experts across the nation. This will be done in a similar manner as the state of California (Miranda, 2007). These experts will be sent machines that represent a completed election. The goal of the security experts will be to hack into the machines and change the vote counts. We will ask each security expert to record information regarding their ability to hack into the machine. If successful, we will ask them to record the time it took them to hack into the machine and their approach. The experts will also compare Prime III's security model to those of the vendors of other DRE systems. After these studies have concluded, Prime III will become available for free download. Our open source model will allow Prime III to be downloaded by anyone, anywhere in the world. Prime III can provide a secure, open source model to assist any nation in their elections. The open source approach should increase scrutiny of the system and provide more solutions to problems. As such, it should also increase voter confidence in the system with the knowledge that Prime III is not a black box system. The type of open source license will be determined at a later date.

## **Conclusion**

Prime III allows voters too confidently cast their ballots in a private and secure environment. A voter can vote using voice, touch or both. This is accomplished by providing a multimodal user interface. The multimodal user interface allows every registered voter to cast their votes equally using one system. This is a major convenience for all voters regardless of ability or disability. Prime III has multiple security measures in place. These include encrypted PDF images of voter ballot files, encrypted PDF imposter files, a secure operating system with advanced security features, video surveillance of each machine's interactions and on site physical security of human poll workers and guards. The shortcomings in today's electronic voting systems such as vulnerability to hackers, malignant workers, faulty code, lack of recount ability, and human error have been addressed in the development of Prime III. Prime III can broaden voter participation in the electoral process by enabling people with various impairments to vote, i.e. visual, auditory, and/or physical, just as any other member of society (107th Congress, 2002). Prime III addresses usable security by providing voters with increased confidence that their votes are actually counted and privacy while casting their vote. Prime III started as a research project (Cross & Gilbert, 2005); however, it is growing into a viable solution to the nation's woes in electronic voting.

## **References:**

- 107th Congress (2002,). "Help America Vote Act". [Online]. [http://www.fec.gov/hava/law\\_ext.txt](http://www.fec.gov/hava/law_ext.txt)
- Cross, E.V. & Gilbert, J.E.: Lets Vote: Multimodal Electronic Voting System. 11th International Conference on Human-Computer Interaction, Las Vegas, Nevada CD\_ROM (2005)
- Feldman, A., Halderman, J., Felton, E. (2006). Security Analysis of the Diebold AccuVote-TS Voting Machine. [Online]. Available: <http://itpolicy.princeton.edu/voting/ts-paper.pdf>
- HBO. (2006). Hacking Democracy. HBO Documentary Films. [Online]. Available: <http://www.hbo.com/docs/programs/hackingdemocracy/synopsis.html>
- "History of Voting Machines". Retrieved November 20, 2004 from [http://www.glencoe.com/sec/socialstudies/btt/election\\_day/history.shtml](http://www.glencoe.com/sec/socialstudies/btt/election_day/history.shtml)
- Hursti, H. (2006). Diebold TSx Evaluation. [Online]. Available: <http://www.blackboxvoting.org/BBVtsxstudy.pdf>

Jones, D. W. (2001). A Brief Illustrated History of Voting. [Online]. Available:  
<http://www.cs.uiowa.edu/~jones/voting/pictures/>

Jones, D. W. (2004), Chad – From waste product to headline. Retrieved November 20, 2004 from THE UNIVERSITY OF IOWA Department of Computer Science web site: <http://www.cs.uiowa.edu/~jones/cards/chad.html>

Kohno, T., Stubblefield, A., Rubin, A. (2004). Analysis of an Electronic Voting System. In: IEEE Symposium on Security and Privacy. Oakland, CA, pp. 27-40

Miranda, N. (2007). "Hackers Hired to Crack Calif. Electronic Voting Machines", Retrieved on July 6, 2007, from [http://abclocal.go.com/kabc/story?section=capitol\\_reports&id=5444235](http://abclocal.go.com/kabc/story?section=capitol_reports&id=5444235).

Optical Scan Voting Systems. Retrieved June 13, 2007 from [http://en.wikipedia.org/wiki/Optical\\_scan\\_voting\\_system](http://en.wikipedia.org/wiki/Optical_scan_voting_system).

Robertson, S. (2004). User-centered interaction design for electronic voting systems. Electronic Voting Project workshop. National Academy of Sciences, Computer Science and Telecommunications Board, Washington, DC.

Security Enhanced Linux. (2006). [Online]. Available at: <http://www.nsa.gov/selinux/index.cfm>

Shamos, M. (2004). "Paper v. Electronic Voting Records – An Assessment". Retrieved on Feb. 03 2007, from <http://www.cfp2004.org/program/materials/p12-shamos.pdf>

"Voting Equipment Summary By Type as of: 11/02/2006". (2006, October) Retrieved June 13, 2007, from [http://www.edssurvey.com/images/File/ve2006\\_nrpt.pdf](http://www.edssurvey.com/images/File/ve2006_nrpt.pdf)