Prime III: Where Usable Security and Electronic Voting Meet

Philicity Williams[1], E. Vincent Cross, II[1], Idongesit Mkpong-Ruffin[1], Yolanda McMillian[1], Kathryn Nobles[1], Priyanka Gupta[1], Juan E. Gilbert[1]

[1] Department of Computer Science and Software Engineering
Auburn University
107 Dunstan Hall
Auburn, AL 36849
{willipk, crossev, mkponio, mcmilym, noblekl, guptapr, gilbert}@auburn.edu

Abstract. Mr. Wilson never votes. He doesn't vote because he is not confident in his reading capabilities; however, he decided that he will vote this year because he heard that blind people will be able to privately cast their vote. He said, "If blind people can vote, then so can I". At the voting precinct, he shows his identification and receives a blank, numbered ballot sheet. He enters a voting booth, placing the ballot into the printer. Using a headset with a microphone, he is able to make his selections by speaking numbers, which gives him confidence that his vote is private. Before printing his ballot, he listens to a summary of his selections. He leaves the voting booth and places his printed ballot into a secure box. Like Mr. Wilson, there are millions of people that don't participate in our electoral process due to disabilities and no confidence in the equipment. Through usable security, Prime III aims to broaden voter participation and confidence.

Keywords: Electronic Voting, Multimodal Interfaces, Human Centered Design.

1 Introduction

America's current voting system is in need of a major overhaul. This became overwhelmingly clear as a result of the 2000 U.S. Presidential election (Celeste et. al., 2005; Rubin, 2006). Accordingly, the federal government has allocated funds for the purchase of modern voting equipment. Electronic voting machines are currently being used in many states. However, the use of these machines has not been without controversy and has met with resistance. For example, it has been widely reported that electronic voting machines pose a number of unacceptable risks such as: vulnerability to hackers, malignant workers, faulty code, lack of recount ability, and human error. Therefore, a system must be built that can address the aforementioned issues and instill voter confidence in the electronic voting process. Also, it is no longer sufficient for such a system to simply be secure; the voter must feel confident in the integrity of the system. Additionally, it should be easy to navigate and use for all segments of the voter population as specified by the 2002 Help America Vote Act (HAVA, 2002).

The system should provide security and trust while being easy to use, e.g. *usable security.*

2 Prime III Voting System

The Prime III voting system was developed using a human-centered computing approach. This approach considers the users first and implements the design that accommodates users. As a result, Prime III is a user friendly electronic voting system which encompasses the necessary security, integrity and user satisfaction safeguards that should be required of all electronic voting systems. It is easily integrated into the current voting process and improves upon it significantly. This provides a degree of familiarity and allows the voter to remain comfortable and confident while using an enhanced voting system.

Prime III is easily integrated into the current voting process. The voter enters the voting precinct and checks in with election officials. After checking in, if printing is desired, the voter is handed a unique ballot card. The voter then takes the ballot card to an empty voting booth. The voting booth contains a touch screen, headset and an empty single sheet printer. The voter places their ballot card into the printer. When the system begins, the voter will cast his/her vote using a *multimodal* (text-to-speech, speech-to-text, touch) user interface. The multimodal interface allows the voter to cast his/her vote using touch or voice, via the touch screen and headset, or a combination of both. Prime III enables voter interaction regardless of their disposition. Voters with visual, hearing or physical impairments can still participate in the electoral process using Prime III. Essentially, if you can't read, see, hear or if you have a physical disability, i.e. arthritis, you can still vote using Prime III in a private, secure, yet usable environment.

The Prime III system has an integrated automatic speech recognizer (ASR) that is accessed through a headset with a microphone. To the best of our knowledge, it is the only electronic voting system that uses audio for input and output in the voting process. Most electronic voting systems use audio for output only. When a voter uses the ASR, they are prompted through the choice of candidates via the headset. Each candidate is assigned a randomly generated number, from which the voter can select by simply saying the number. The first candidate is assigned a random number and incremental numbers are assigned for each subsequent candidate. This approach ensures voter privacy. Eavesdroppers will here a voter speaking numbers with no indication of the voter's choices. This provides an easy to use, private audio interface for voice voting. After the voter finishes voting, their selections are displayed on the screen and spoken to them as well. At this point, the voter is required to confirm their selections using touch or speech. Upon review and confirmation from the voter, the system writes the ballot to disk and prints out the corresponding ballot card (if printing is enabled). If printing is used, the voter will receive a printed copy of the ballot. The printed ballots provide a redundant paper trail of the vote, should there be a need for a recount. However, some precincts don't require paper trails or simply don't want the hassle of paper trails. Therefore, Prime III provides the functionality to determine whether printing will be enabled or not for the precinct. Next, the voter exits the voting booth and places their ballot card into the ballot box, if printing was used. This entire process is open to the public and highly visible as the voting area is surrounded by glass walls or simply no walls. The voters can view the machines, the ballot box, guards, and each other. Essentially, the voters become additional security staff while in the precinct. The only hidden aspects of the system are the actual touch screens and printed ballots.

3 Prime III Voting System Security Model

Prime III runs on a Security Enhanced Linux, SELinux (Security Enhanced Linux, 2006), operating system. SELinux was developed by the National Security Agency as an implementation of mandatory access control using Linux Security Modules (LSM) in the Linux kernel, based on the principle of least privilege. From NSA, "NSA Security-enhanced Linux is a set of patches to the Linux kernel and some utilities to incorporate a strong, flexible mandatory access control (MAC) architecture into the major subsystems of the kernel. It provides a mechanism to enforce the separation of information based on confidentiality and integrity requirements, which allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can be caused by malicious or flawed applications." (Security-Enhanced Linux, 2006) SELinux provides advanced access controls and logging capabilities. Prime III uses the access control features to restrict access of an authorized login, based on the security policy configuration, for each system.

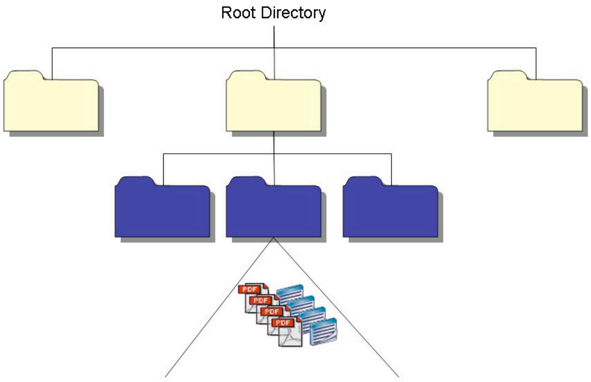

Figure 1: Imposter File Organization on Prime III

The logging features in SELinux are used for post election auditing, if necessary. On top of the SELinux operating system, 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 1.

Under the root directory, there are several imposter folders, each with different names and no identifiable pattern in the names. Each folder contains 500 subfolders. Each subfolder contains portable document format (PDF) images of voter ballots and encrypted ballot files. These are identical to the printed ballots that contain only the voter's selections. Each ballot, whether printed, in PDF or encrypted contains a date time stamp of when the ballot was cast. The PDF and encrypted 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 PDF and encrypted 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 the real or an imposter, is encrypted with Triple Data Encryption Standard (Triple-DES), Advanced Encryption Standard (AES) or both encryption algorithms. The encryption method used for the imposter files are randomly selected. As such, the imposter files have not only random layout/structure but along with that randomly selected encryption/decryption method. The input key is used to determine the real vote file's layout/structure, encryption method and encryption folder. 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 a haystack.

3 Conclusion

Prime III has the requisite capabilities to provide the nation with a private, secure and usable electronic voting system. 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 (HAVA, 2002). 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. Currently, Prime III is undergoing usability testing with people from various demographics, e.g. elderly, disabled, etc. Additional security studies will be conducted where security experts are given Prime III voting machines and asked to change the vote counts. These experiments will inform the Prime III security model. After the usability and security studies are completed, Prime III will be available for download and additional testing will be conducted by election officials.

References

1. Celeste, R.F., Thornburgh, D., & Lin, H.: Asking the Right Questions About Electronic Voting. National Academy Press (2005)
2. 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)
3. Help America Vote Act (HAVA). Public Law 107-252, 107.Congress United States of America. http://www.fec.gov/hava/hava.htm (2002)
4. Rubin, A.: Brave New Ballot: The Battle to Safeguard Democracy in the Age of Electronic Voting. Morgan Road (2006)

Bios:

Ms. Philicity Williams is a Ph.D. student in the computer science and software engineering department at Auburn University. Her research interests are in databases, data mining and human centered computing.

Mr. E. Vincent Cross, II is a Ph.D. student in the computer science and software engineering department at Auburn University. His research interests are in human-robot interaction and human centered computing.

Mrs. Idongesit Mkpong-Ruffin is a Ph.D. student in the computer science and software engineering department at Auburn University. Her research interests are in information security and human centered computing.

Ms. Yolanda McMillian is a Ph.D. student in the computer science and software engineering department at Auburn University. Her research interests are in human centered computing with an emphasis in interfaces for people with disabilities.

Ms. Kathryn Nobles is a Ph.D. student in the computer science and software engineering department at Auburn University. Her research interests are in educational technologies and human centered computing.

Ms. Priyanka Gupta is a Ph.D. student in the computer science and software engineering department at Auburn University. Her research interests are in usability and human centered computing.

Dr. Juan E. Gilbert is the TSYS Distinguished Associate Professor in the computer science and software engineering department at Auburn University where he directs the Human Centered Computing Lab. Dr. Gilbert has research projects in Spoken Language Systems, Advanced Learning Technologies, User Interfaces (Usability), Ethnocomputing (Culturally Relevant Computing) and Databases. He is also a Senior Member of the IEEE Computer Society, he serves on the IEEE Board of Governors and he is the Editor for the new Broadening Participation in Computing Series in Computer for IEEE Computer Society.