Remote Poll-Site Voting

Submission for Phase I

by

Parth P. Vasa
Soo-Yung Cho
Jeremy Mullendore
Bodhisattva Debnath

This report is divided into two sections. Section A(2-5) deals with the literature survey and briefly describes past and current work on the subject of electronic voting systems. Section B(6-7) lists our system requirements.

A) Literature Review

Given Below is a summary of the 16 papers from different aspects of on electronic voting systems. From large amount of information we have selected a few papers, which touch upon different fields of Internet/Electronic voting. The papers at the start are comprehensive reports by government organizations, which provide broad and deep coverage of social and technical aspects of Internet Voting. After that there are some highly readable and informative papers that look at the problem from different angles. Following these are some heavy duty cryptography papers of proposed schemes of Internet voting.

1. Report of the National Workshop on Internet Voting

This report contains an overview of the electronic voting process - its methods, requirements, issues, and feasibility. This report contains what we find to be the most complete list of requirements for electronic voting. As such, these requirements are outlined in the requirements section of this document. The requirements for election systems are: Eligibility and Authentication, Uniqueness, Accuracy, Integrity, Verifiability and Auditability, Reliability, Secrecy and Non-Coercibility, Flexibility, Convenience, Certifiability, Transparency, and Cost-effectiveness. The report concludes that poll-site electronic voting is feasible in the near future. Remote Internet voting systems and Internet-based voting systems, however, pose extreme risks to the voting process and should not be put in place until many issues are resolved.

2. Caltech - MIT report on Voting

This report describes the inadequacies of current voting technology and proposes a multi-pronged strategy for voting to address the current inadequacies. The authors talk about registration problems and call for centralization of voter registration databases across a state, among other suggestions. The authors also touch upon poll site staffing practices, financing, and ballot security and finally propose a new system of remote poll-site voting.

The authors stress that almost all vote tallying software should be open source whereas the interface should be proprietary. The authors draw a distinction between capturing voters' intentions, confirming vote selections and casting votes. Each step above should be serviced by different systems. The authors maintain that previously these steps were seen as one, leading to the design of overly complex monolithic systems that were hard to certify.

3. California Internet Voting Task Force - A Report of feasibility of Internet Voting

This Report starts by describing what is Internet voting and a brief history and evolution of electronic voting. The report then goes on to describe the issues in implementation of Internet Voting. Task force recommends an incremental approach, divided in 4 stages by which the Internet voting (i-voting) can be achieved. Starting from i-voting from Voter’s polling place in stage one, the last and final stage goes for fully remote Voting from any Internet connection. The most relevant stage of these

(to our project) is the stage two (i-voting from Any Polling place). The report also clearly explains the issues before, during and after voting.

After describing the detailed requirements of i-voting, the report discusses the possible usefulness and impact of Internet voting. It states that the convenience provided my Internet voting might increase the voter turnout. However they also state that a large number of citizens, especially the people above the age of 55 are still skeptic about the concept.

4. Avi Rubin - Security Considerations for Remote Electronic Voting over the Internet

This paper discusses the security considerations for remove electronic voting in public elections. The author clearly explains, why such a lucrative and convenient looking option of Remote Internet Voting is so difficult (way beyond our reach at present) to achieve. Some of the major issues he discusses include the issues with malicious payload such as viruses and remotely controlled software (such as BO2k), attacks on communication infrastructure, social engineering etc. In concluding remarks Dr. Rubin points that though there is still hope, at the present time, we are not ready for Remote Internet voting.

5. Lorrie Faith Cranor : Electronic Voting: Computerized polls may save money, protect privacy

In this very readable Article the author describes Internet voting and protocols used for it. The article starts with describing the requirements for such a system. The author then describes some protocols for Internet voting, starting from a simple protocol and finally showing the use of blind signature for Internet Voting.

6. Jim Adler – Security Versus Compatibilty in Online Elections

This short paper discusses a different aspect of Online Elections. The author starts by describing an "Attack Tree" of how the ballot can be compromised. In rest of the paper author describes the usefulness and importance of encryption at client side. This means that the client side component (dubbed browser here) should be having the capability of performing mathematical functions needed for encryption. Usually the browsers support encryption on the web. Which protects against in-transit attacks but doesn't foil the attacks of a system level attacker at the browser or the server end.

7. Jim Adler - Internet Voting Primer

Here the author describes in very simple terms what makes up e-voting and what are the requirements. Also shown are the comparisons of requirement between a few election systems such as E-commerce, Trusted Authority, Individually Verifiable, Universally verifiable etc.

8. Michael Ian Shamos - Electronic Voting – Evaluating the Threat

Proposed here is a method of evaluating security measures for countering threats to computerized election systems. It sets forth six system requirements (called commandments), that society and legislatures mandate. The election process is

considered as divided in two parts, capturing the voter preferences reliably and reporting them accurately. In later parts of the paper the Author stresses on the need of the election software being open source and being subject to heavy duty testing. One other prominent aspect of the paper is the focus upon rationally evaluating the risk factors of electronic voting.

9. Peter G. Neumann - Security Criteria for Electronic Voting

In this paper the author paints a bleak picture of electronic voting and justifies it. He discusses the usual requirements of an electronic voting system and then talks about what can be realized. He talks about how system accountability can be subverted by system code that operates below the accounting layers and emphasizes open code. He further talks about system availability and system robustness and says that these aims are not easily achievable, giving examples of how systems can fail. He also draws attention to the quality level of current software and says that developing high assurance software systems is too expensive for companies.

10. Douglas Jones - E-Voting: Prospects and Problems

This article presents a couple of interesting security issues with regards to electronic voting systems. First, the author outlines the possible downside to the use of proprietary code (Trojan Horses, etc.). The author recommends the institution of an independent testing authority and/or the use of open source components. The second issue presented is software version control and the question of how one knows whether the program binary running on a voting machine is the same as the code that was inspected. Jones suggests that a third party archive the code, its equivalent binary, and the compiler used to create so that future checks can always be done.

11. Irwin Mann - Open Voting Systems (CFP '93)

This article presents a paradigm for public access to the accountability of the voting process, called an "open voting system." Mann defines an open voting system as one where every hardware and software component is in the public domain, there is independent monitoring of software, and public monitoring of the system for problems is institutionalized.

12. Mark Herschberg - Secure Electronic Voting Over the World Wide Web

This Master's Thesis details an implemented, functioning electronic voting system based on the scheme presented in "A Practical Secret Voting Scheme for Large Scale Elections" by Fujioka, Okamoto, and Ohta. Unlike past schemes based on Fujioka, et al., Herschberg's does not rely on a public key system (Sensus) nor does it open itself up to hackers' altering the system on the end-user's (voter's) machine as the code is written in Java (which has the Sandbox model). A few problems with this system are that it has a single point of failure in the communications and it leaves itself open to the possibility of spoofing attacks.

13. Cramer, et al. - A Secure and Optimally Efficient Multi-Authority Election Scheme

This paper presents a multi-authority secret-ballot election scheme that guarantees privacy, universal verifiability, robustness, and both computational and information-theoretic privacy. The complexity of this scheme is optimal with respect to the voter and the authorities.

14. **Josh Cohen Benolah, Moti Yung – Distributing power of a Government to enhance the Privacy of Voters.**

This paper describes a scheme to distribute the power of government (tellers) in the election system. It is claimed that this kind of scheme will enhance the confidence in elections held in un-trusted environments. The scheme achieves that even if a single teller is honest, there can be no fraud of leakage of privacy, with a very high probability

15. **David Clausen, Daryl Puryear, Adrian Rodriguez - Secure Voting Using Disconnected, Distributed Polling Devices**.

Presents a system for secure electronic voting, which does not rely on persistent network. Instead it is designed to work in a disconnected (or more accurately "intermittently connected") environment. Also given is a real life implementation of a truly electronic election conducted as a test case at Stanford University. The paper describes each process of the test election.

16. **Michael Radwin: An untraceable, universally verifiable voting scheme**

In this paper author describes a voting scheme with properties of verifiability, convenience and intractability. The proposed scheme uses Chaum's blind signature algorithm. These algorithms have acceptance in the field of digital cash. It uses blinded signature using a PKI similar to RSA. Furthermore the scheme is enhanced to prevent double voting (similar to double spending). This is achieved by an interactive protocol based on reveling some secrets at each stage.

B) Requirements

While performing our literature survey, we found many lists of criteria for voting systems. The list of criteria found in "Report of the National Workshop on Internet Voting" by the Internet Policy Institute, however, seems to be the most complete around. In fact, we could find only one additional requirement not outlined in this report. The Institute's criteria are the following: eligibility and authentication, uniqueness, accuracy, integrity, verifiability and auditability, reliability, secrecy and non-coercibility, flexibility, convenience, certifiability, transparency, and cost effectiveness. We have added to this list "availability." This was found in the paper "Security Criteria for Electronic Voting" by Peter G. Neumann. In the following paragraphs. we will touch briefly on each of the criteria.

The first requirement of any election system is eligibility and authentication. In order for an election to be fair and accurate, only voters who are eligible to vote can be registered to do so. For instance, if the local laws state that criminals or convicted felons cannot vote, then the election system must insure that they do not. Also, before an individual is allowed to vote, he/she must be authenticated as the person he/she claims to be and as an eligible, registered voter.

Uniqueness refers to the requirement that no individual should be allowed to cast more than one vote. Obviously, "one person, one vote" is a general rule of democracy that needs to be upheld.

Accuracy is another obvious requirement of an election system. All votes need to be recorded and tabulated correctly for an election system to be worth anything.

Another requirement of systems is integrity. When an individual casts his or her vote, he/she should be sure that that vote will be counted as cast. No one should be able to modify, forge, or delete a vote. Obviously, this means that the voting machines should be tamperproof, not just the software.

Verifiability and auditability are important in any voting system and extremely important in an electronic system. In order for the public to be sure that an electronic system is working correctly, they need to verify that all votes (especially their own) have been counted and that there is a "paper trail" for recounts.

Even in an electronic setting, election systems need to be reliable. No votes should be lost during an election, even if there are power outages, network outages, hard drive crashes, or any other failures. Obviously, robustness of computer systems is a very difficult challenge. However, for a voting system to be useable, it needs to be as reliable and robust as possible.

Similarly, voting systems need to be available. An election should not be slowed or postponed by loss of some service like a network. Protections need to be made to help insure that the system remains up and active during its designated operational time (i.e. - throughout election day) and that malicious attacks like
denial of service do not ruin an election.

Another important criterion of an election system is that votes be secret. The selections of a voter should be personal information that is not accessible by anyone - even election officials and administrators. This insures that no one can be coerced into voting a certain way and that no one can be punished for a certain vote

(imagine a foreign "democracy" where a person who votes against the ruling faction is jailed or worse).

The interface of an election system is another item of importance. A good election system should allow for a variety of ballot styles and formats and should run on multiple platforms. Above all, it should be accessible to the everyone - the handicapped, the elderly, the poorly educated, etc.

On the same note, election systems should also be convenient. A voter should be able to cast his or her vote quickly and with a minimum of skill and technical knowledge.

Certifiability is an important requirement to the government and the public alike. All systems should be testable so that officials and the public have confidence that they perform as they were designed. It is with this idea that many individuals state that all voting systems should be open source and open architecture. This allows for election officials, voters' rights groups, and individual citizens to examine the election system and process and find flaws.

In addition, voting systems need to be transparent to the users. Voters should be able to have a general idea of how the voting process works.

Finally, election systems need to be cost-effective. A system could be the most secure, reliable, accurate, and user-friendly in the world, but it will not be used unless it is affordable to most towns, counties, and states.

To summarize, we have outlined a set of functional and security requirements for electronic voting. Among the functional requirements are eligibility and authentication, uniqueness, accuracy, verifiability and auditability, flexibility, convenience, transparency, and cost-effectiveness. The security requirements include integrity, authentication, reliability, availability, and secrecy and non-coercibility. Obviously, some of these requirements like authentication and auditability can be viewed as both functional and security in nature. We simply chose the category that seems most fitting to us.

In general, we feel that all of the above requirements need to be met to have a perfect voting system. However, realistically this is not possible. A computer system can never be completely reliable. Outages will occur and these can be dealt with, but scenarios like hard drive crashes are harder to deal with and recover from without loss of vote(s). In the same vein, system availability may also be compromised if large network or power outages occur. As we all know, these things happen. Gas powered generators at every poll location could remedy the problem of power outages, but this is a highly expensive and, thus, unfeasible solution. Thus, with our system we will attempt to fulfill all of the requirements identified in this paper excepting reliability and availability. These requirements are simply too difficult and too expensive to fully realize. However, we plan to design our system to take care of all but the very worst scenarios in regards to reliability and availability.