Electronic Voting - A Survey

Prashanth P. Bungale and Swaroop Sridhar
Department of Computer Science
The Johns Hopkins University

As the world watched the electoral drama unfold in Florida at the end of 2000, people started wondering, "Wouldn't all our problems be solved if they just used Internet Voting?". People all over the world soon started taking a hard look at their voting equipment and procedures, and trying to figure out how to improve them [1]. There is a strong inclination towards moving to Remote Internet Voting – at least among the politicians – in order to enhance voter convenience, increase voter confidence and voter turnout. However, as will be seen later in this paper, there are serious technological and social aspects that make Remote Internet Voting infeasible in the visible future. Therefore, many technologists have suggested that remote poll-site electronic voting, where the voter can vote at any poll-site (not only his home county poll-site), seems to be the best step forward as it provides better voter convenience, but at the same time, does not compromise security. This paper presents a survey of the state of the art in Electronic Voting, including the various works done in Internet Voting (and the arguments against its use), as well as in electronic poll-site voting.

Electronic voting refers to the use of computers or computerized voting equipment to cast ballots in an election. Sometimes, this term is used more specifically to refer to voting that takes place over the Internet. Electronic systems can be used to register voters, tally ballots, and record votes [2].

The Caltech/MIT Voting Technology Project [3] came into being in order to develop a new voting technology in order to prevent a recurrence of the problems that threatened the 2000 U. S. Presidential Elections. The report assesses the magnitude of the problems, their root causes and how technology can reduce them. They address a wide range of "What is" issues including voting procedures, voting equipment, voter registration, polling places, absentee and early voting, ballot security, cost and public finance of elections, etc. They then propose a novel "What could be" framework for voting technology (that moves away from monolithic voting structures), and propose that a process for innovation be setup. The framework is "A Modular Voting Architecture ("Frogs")" [4,5,6] in which vote generation is performed separately from vote casting, and the "Frog" forms a permanent audit trail, the importance of which cannot be over-stressed. Here, the vote generation machine can be proprietary whereas the vote casting machine must be open-source and thoroughly verified and certified for correctness and security. Finally, the report provides a set of short-term and long-term recommendations on the various issues related to voting.

In "Electronic Voting" [7], Rivest addresses some issues like the "secure platform problem" and the (im)possibility of giving a receipt to the voter. He also provides some personal opinions on a host of issues including the striking dissimilarity between e-commerce and e-voting, the

dangers of adversaries performing automated, wide-scale attacks while voting from home, the need for extreme simplicity of voting equipment, the importance of audit-trails, support for disabled voters, security problems of absentee ballots, etc.

The NSF Internet Voting Report [8] addresses the feasibility of different forms of Internet voting from both the technical and social science perspectives, and defines a research agenda to pursue if Internet voting is to be viable in the future. It groups Internet voting systems into three general categories as follows:

- *Poll-site Internet voting*: It offers the promise of greater convenience and efficiency in that voters could cast their ballots from any poll site, and the tallying process would be both fast and certain. More importantly, since election officials would control both the voting platform and the physical environment, managing the security risks of such systems is feasible.
- *Kiosk voting*: Voting machines would be located away from traditional polling places, in such convenient locations as malls, libraries, or schools. The voting platforms would still be under the control of election officials, and the physical environment could be modified as needed and monitored (e.g., by election officials, volunteers, or even cameras) to address security and privacy concerns, and prevent coercion or other forms of intervention.
- *Remote Internet voting*: It seeks to maximize the convenience and access of the voters by enabling them to cast ballots from virtually any location that is Internet accessible. While this concept is attractive and offers significant benefits, it also poses substantial security risks and other concerns relative to civic culture. Current and near-term technologies are inadequate to address these risks.

The report presents some findings on the feasibility of each of these categories and provides research recommendations for the long-term future. It then identifies criteria for election systems. Finally, it addresses the technological issues (including voting system vulnerabilities, reliability, testing, certification and standards, specifications of source code, platform compatibility, secrecy and non-coercibility, etc.) and social science issues (such as voter participation, voter access, the election process, voter information, deliberative and representative democracy, community and character of elections, distribution of roles, legal concerns, voter registration, etc.)

The California Internet Voting Report [9] suggests a strategy of evolutionary rather than revolutionary change towards achieving the goal of providing voters with the opportunity to cast their ballots at any time from any place via the Internet. The report defines four distinct Internet voting models – Internet voting at voter's polling place, Internet voting at any polling place, Remote Internet voting from County computers or kiosks, Remote Internet voting from any Internet connection – and the corresponding technical and design requirements that must be met when implementing any of the stages. It addresses the advantages, implementation and security issues of each of the four stages. They believe that additional technical innovations are necessary before remote Internet voting can be widely implemented as a useful tool to improve participation in the elections process and that current technology however would allow for the implementation of new voting systems that would allow voters to cast a ballot over the Internet from a computer at any one of a number of county-controlled polling places in a county. Finally,

the report presents the findings and recommendations of the task force on policy issues. The Appendix A [10] of this report contains a technical analysis of the communication and security issues inherent in Internet voting, along with recommended privacy and security requirements for any Internet voting systems. It also deals with potential Internet-based voter registration systems and, briefly, with Internet petition-signing systems as well.

An extensive survey of e-voting technology has been provided in "e-Voting Security Study" [11]. It provides a survey of recent academic and commercial projects in the area, in addition to the area's prominent academics' personal views and testimonies regarding the issues. It identifies threats, potential sources of attack and possible methods of attack in such voting systems. It also identifies security objectives and requirements of an electronic voting system.

The foundation of much of the academic work in the area of remote voting is a paper by Fujioka, Okamoto and Ohta (FOO) [12]. It gives a mathematical framework for a secure election that involves an administrator, and a counter and the voter connected by an anonymous channel. Practically focused projects build on the blind voting protocol proposed in this paper. Sensus [13] uses blind signatures to ensure that only registered voters can vote and that each registered voter votes exactly once, while at the same time maintaining voter's privacy. It allows voters to verify independently that their votes were counted correctly and anonymously challenge the results, should their votes be miscounted. Another project called E-VOX [14] at MIT implements a simplified, user-friendly version of the FOO framework using Java, Netscape and JDBC (Java Database Connectivity). This system is still involved in teaching and research and was used for an Undergraduates Association election at MIT in 1999. "Multiple Administrators for Electronic Voting" [15] improves this further by distributing the authority among multiple administrators to prevent vote forging.

"An untraceable, universally verifiable voting scheme" [16] presents a remote voting scheme that applies the technique of blinded signature to a voter's ballot so that it is impossible for anyone to trace the ballot back to the voter. They achieve the desired properties of privacy, universal verifiability, convenience and untraceability, but at the expense of receipt-freeness.

The E-Poll (Electronic Polling System for Remote Voting Operations) project [17] investigates broadband mobile communications based on the UMTS standard for providing the E-Poll network with the required bandwidth and security. This makes it possible to use E-Poll kiosks anywhere, within a private, reliable and protected network. The voter-recognition system is based on an innovative smart card with an embedded biometric fingerprint reader, which performs voter recognition with absolute security. An ergonomic kiosk facilitates use by disabled people.

The FREE e-democracy project [18] is dedicated to creating the GNU.FREE Internet Voting system and also advocating Free Software, which is non-partisan and non-commercial in origin.

[19] presents a system for secure electronic voting which does not rely on persistent network connections between polling places and the vote-tallying server. They build the system on a disconnected (or, more accurately, an intermittently connected) environment, which behaves well in the absence of network connectivity.

"Security Criteria for Electronic Voting" [20] considers some basic criteria for confidentiality, integrity, availability, reliability, and assurance for computer systems involved in electronic voting. After an assessment of the realizability of those criteria, it concludes that, operationally, many of the criteria are inherently unsatisfiable with any meaningful assurance.

In [21], Rubin identifies the new risks brought about by introducing the state-of-the-art technology into the election process, which may not be worth taking. The major security risks identified include those at the voting platform – including malicious payload (attack programs, remote administration and monitoring toolkits, etc.) and delivery mechanism (worms, viruses and bugs, active content downloaded automatically, etc.) – and the communications infrastructure – including (distributed) denial of service attack, DNS server attack, etc. He also identifies security issues in social engineering and in using specialized devices.

Discussions on requirements, threat perceptions and socio-political issues regarding electronic voting can be found in [22, 23, 24, 25, 26].

References

[1] "*Voting After Florida: No Easy Answers*," Lorrie Faith Cranor, December 2000, http://lorrie.cranor.org/.

[2] "*Electronic Voting*," Encyclopedia of Computers and Computer History, prepared by Lorrie Faith Cranor and edited by Raul Rojas, published by Fitzroy Dearborn, 2001.

[3] "*Voting – What is, What Could be*," Caltech/MIT Voting Technology Project (VTP) Report, July 2001.

[4] "*A Modular Voting Architecture ("Frogs")*," Shuki Bruck, David Jefferson, and Ronald L. Rivest, August 2001.

[5] "*Comments of Professor Ronald L. Rivest*", Caltech/MIT VTP Press Conference, July 16, 2001, http://theory.lcs.mit.edu/~rivest/publications.html.

[6] "*Testimony given before the U.S. House Committee on Administration*", Ronald L. Rivest, May 24, 2001, http://theory.lcs.mit.edu/~rivest/publications.html.

[7] "*Electronic Voting*," Ronald L. Rivest, Technical Report, Laboratory for Computer Science, Massachusetts Institute of Technology.

[8] "*Report of the National Workshop on Internet Voting: Issues and Research Agendas*," Internet Policy Institute, Sponsored by the National Science Foundation, Conducted in cooperation with the University of Maryland and hosted by the Freedom Forum, March 2001.

[9] "*A Report on the Feasibility of Internet Voting,*" California Internet Voting Task Force, January 2000.

[10] "*Appendix A: Technical Committee Recommendations*," California Internet Voting Task Force, January 2000.

[11] "*e-Voting Security Study*," E-Democracy Consultation, U. K. Cabinet Office, http://www.edemocracy.gov.uk/library/papers/study.pdf.
[12] "*A Practical Secret Voting Scheme for Large Scale Elections*," A. Fujioka, T. Okamoto, and K. Ohta, Advances in Cyptology - AUSCRYPT '92.
[13] "*Sensus: A Security-Conscious Electronic Polling System for the Internet*," Lorrie F. Cranor and Ron K. Cytron, Proceedings of the Hawai`i International Conference on System Sciences, January 7-10, 1997, Wailea, Hawai`i, USA.
[14] "*Secure Electronic Voting Over the World Wide Web*," Master's Thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, May 1999.
[15] "*Multiple Administrators for Electronic Voting*," Bachelor's Thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, May 1999.
[16] "*An Untraceable, Universally Verifiable Voting Scheme*," Professor Philip Klein, Seminar in Cryptology, December 12, 1995.
[17] http://www.e-poll-project.net/
[18] http://www.free-project.org/
[19] "*Secure Voting Using Disconnected, Distributed Polling Devices*," David Clausen, Daryl Puryear and Adrian Rodriguez, Department of Computer Science, Stanford University.
[20] "*Security Criteria for Electronic Voting*," Peter G. Neumann, 16th National Computer Security Conference, Baltimore, Maryland, September 20-23, 1993.
[21] "*Security Considerations for Remote Electronic Voting*," Aviel D. Rubin, Communications of the ACM, Vol. 45, No. 12, December 2002.
[22] "*Ten Things I Want People to Know About Voting Technology*," Kim Alexander, President and Founder, California Voter Foundation, Presented to the Democracy Online Project's National Task Force, National Press Club, Washington, D. C., January 18, 2001.
[23] "*Electronic Voting – Evaluating the Threat*," Michael Ian Shamos, International Conference on Computers, Freedom, and Privacy, Burlingame, California, 1993.
[24] "*Internet Voting: Will it Spur or Corrupt Democracy?*," Lance J. Hoffman, Technical Report, Computer Science Department, The George Washington University, Washington, D. C.
[25] "*Online Voting*," postnote – a publication of the U. K. Parliamentary Office of Science and Technology, May 2001.
[26] "*Evaluating Voting Technology*," Douglas W. Jones, Testimony before the United States Civil Rights Commission, Tallahassee, Florida, January 11, 2001.