Rashidat Agbaje
JaTara Brown
600.443
February 20, 2003

Survey of Literature

Introduction

Much work has been done in recent years to switch the current election system to an Internet voting system that would be convenient to all. With the rise of technology everywhere, the natural progression of thought is adapting that technology for use in an important component of our lives – our electoral system. The 2000 presidential election fiasco in Florida has only highlighted the need to produce an Internet voting system that would avoid or eliminate such situations. Many experts have been asked to join task forces and give invited lectures on the prevailing issues that surround Internet voting. Our report details their observations and conclusions.

Advantages and Disadvantages

Remote poll site electronic voting has many advantages. The most obvious advantage is that of near instantaneous counting and tallying of votes, thereby eliminating the human error factor. Machines can add up votes in a fraction of the time that it would take for humans to the same task, usually with more efficiency and better accuracy.

Also, it's a step towards the ultimate in voting technology – remote Internet voting. It eliminates the needs for absentee ballots, which are know to be highly insecure and unreliable. There is no paper trail, with the exception of those

systems that print out individual ballots for auditing purposes. That means no tons of paper to store and protect for an indefinite period of time. In addition, there is a reduction in the amount of lost votes or miscounts.

A very important advantage of electronic voting is the reduced voter ambiguity in some cases. Because the ballot is electronic, there is no need for a human being to interpret the difference between a dangling/dimpled/pregnant chad or between two marked ovals in an optical ballot. Neither does any human being have to decipher the sometimes unreadable handwriting of a voter who elects to write-in their vote.

However, this system is not without its disadvantages. There is a possibility of system or mechanical failure, which can lead to lost votes. There is also the possibility of external attacks, usually due to hacker mischief such as denial of service (DoS) attacks. Generally, the problem is primarily that of securing the system and ensuring that the election overall is fair and impartial.

The “weakest link” in the current process is voter registration. Counties will have to be able to authenticate voters not voting in their home county. Therefore, the voter registration database must be as up-to-date and accurate as possible and shared between counties and states, which is not always the case with the current system.

Also, it is a given that new technological breakthroughs occur consistently every year. However, many cash-strapped counties may resist purchasing machines for several years because they cannot afford the cost to upgrade their systems. This inequity results in systems that vary according to reliability and

security from county to county. There is not only the initial expense involved in the purchase of such systems, but there is also the storage and maintenance cost incurred in-between and during elections. Since these costs are usually incurred directly from the county's budget, even these simple necessary costs may be sacrificed in order to divert money to other county programs which need the funds badly.

There is no federal mandate for a paper trail to be required, hence in some cases there is no way to audit a system or handle a recount if one is required. In such cases, a time-consuming and expensive revote may be necessary.

Special Considerations

There are many technical and social issues that need to be taken into consideration in a discussion about remote poll site voting. In terms of social issues, this system should still be in compliance with federal and state/local laws that are in place for the current election process. There is the issue of the "digital divide," a well-known and well-researched phenomenon which explores the fact that minorities such as Blacks and Hispanics are less likely to have access to technological advances as opposed to affluent Whites or Asians. By federal mandate, the system must be accessible to everyone. An all-electronic election system may disenfranchise such voters and effectively prevent them from fully participating in the democratic process.

The important thing to remember is that everyone, while they are not required to vote, should be able to choose among available methods of voting and be able to cast a valid ballot. All voters have the right to be free from vote selling,

vote coercion or vote solicitation while they are participating in the electoral process. Sometimes systems are not sensitive to the needs of people with disabilities at times. If the system is not equipped with Braille labels or audio prompts, blind voters require a sighted volunteer to assist them through the process, thereby robbing them of their right to vote privately. Also, some machine designs may not be as readily accessible to wheelchair-bound persons, also requiring them to give up their privacy for the assistance of a volunteer to help them cast their votes.

Of all of the social issues, trust and integrity are paramount. Since voting is at the heart of our republican form of government, it is important that voters be able to have faith in the system and believe they have been a part of the democratic process. Even the most secure, the most reliable, the most accurate voting system can be rendered worthless if the voters do not believe in the system and its ability to handle the election process fairly and impartially. Hence, it is important when designing a system to keep these social issues in mind. Ultimately, the voter should feel as though that the system ensures fairness and secures the democratic process.

The primary technological issue has to do with security, which is a very important part of the election process. Any system is only as strong as its "weakest link," whether that weak link is in the machines themselves, over the communication network, on the central server or any other aspect of the system. There must be measures in place to ensure that people do not "beat" the system by casting multiple or otherwise ineligible votes or by tampering with votes already

cast by eligible voters. Programmers can program the system to behave differently from expected behavior or they can accidentally leave security holes for a hacker to exploit. If some form of networking is used, then that means of communication must be secured as well to prevent "man-in-the-middle" attacks from hackers. Currently, there is no existing voting system that meets the stringent requirements for security.

The logistics of the system must also be considered. There should be a means of ensuring that not only each voter is authorized and thus eligible to vote, that each voter only casts one vote. This is accomplished by a strong and accurate voter registration system, something that does not yet exist today. There have been documented cases of dead voters participating in the election process as well as voters taking advantage of loopholes to place multiple votes for their favorite candidate. Clearly, the overall electoral system needs to examined and strengthened from beginning to end.

Conclusion

There are many ongoing debates about the future of electronic voting. Many of these papers are clear on one fact: remote poll site electronic voting, with significant modifications, is indeed a viable choice for voting in the 21st century. However, remote voting via the Internet is not yet a suitable choice due to many weak, exploitable points at various locations in the system, including the Internet itself. Still, these papers are optimistic that at one point in the future, when the major security issues have been addressed, that Internet voting will become as widespread prevalent as many of our other Internet activities, such as banking.

Bibliography

Elliott, David M. "Examining Internet Voting in Washington." Washington Secretary of State's Office. White Paper. 1999 (http://www.electioncenter.org/voting/InetVotingWhitePaper.html).

Federal Voting Assistance Program, Department of Defense Voting Over the Internet (VOI) Pilot Project (http://www.fvap.gov/voireport.pdf).

Internet Policy Institute. "Report of the National Workshop on Internet Voting: Issues and Research Agenda." National Science Foundation, March 2001 (http://www.netvoting.org/Resources/InternetVotingReport.pdf).

Jones, Bill. "California Internet Voting Task Force: A Report on the Feasibility of Internet Voting." January, 2000 (http://www.ss.ca.gov/executive/ivote/).

MIT and CalTech Voting Technology Project in July 2001 (http://web.mit.edu/voting/).

Rubin, Avi. "Security Considerations for Remote Electronic Voting over the Internet." November 2000 (http://www.avirubin.com/e-voting.security.html).

Smith, Van. "Future Vote: Computerized Balloting is Taking Over Elections in Maryland – But Can We Trust the Results?" Baltimore Citypaper Online Dec 11-17, 2002 (http://www.citypaper.com/2002-12-11/pf/feature_pf.html).

Smith, Van. "Ballot Check: Computerized Voting Comes Under Fire in Georgia and California" Baltimore Citypaper Online Feb 19-25, 2003 (http://www.citypaper.com/current/pf/mobs2_pf.html).

Smith, Van. "The Vote Counters: Computerized Ballot-Counting Systems Under Fire" Baltimore Citypaper Online Oct 30-Nov 5, 2002 (http://www.citypaper.com/2002-10-30/pf/mobs2_pf.html).