David Friedman
Charles Wright
Dan Kalowsky
John Daniel

Electronic Voting Literature Review

Computer scientists who have done work in, or are interested in, electronic voting all seem to agree on two things:

- Internet voting does not meet the requirements for public elections
- Currently widely-deployed voting systems need improvement

Voting on the Internet using everyday PC's offers only weak security, but its main disadvantages are in the areas of anonymity and protection against coercion and/or vote selling. It's such a truly bad idea that there seems to be no credible academic effort to deploy it at all. The Presidential elections of 2000 brought national attention to problems with current American methods of casting and counting votes in public elections. Most people believe that the current system should be changed; there is much disagreement on *how* such changes should be made.

The MIT/Caltech researchers [1] "see a promising future for electronic voting, despite its problems today" (under a few conditions). They advocate using the methods currently in use which result in the lowest average numbers of "uncounted, unmarked, and spoiled ballots," like in-precinct optical scanning. Their report even proposes a framework for a new voting system with a decentralized, modular design.

Other researchers have done work in electronic voting; while they may not explicitly mention voting from remote poll sites, their work is nonetheless relevant to any effort at designing or implementing a remote poll site voting system. Lorrie Cranor [2] could be classified, like the Caltech/MIT researchers, as a cautious optimist. She acknowledges the problems inherent in each kind of voting apparatus, but doesn't make an overt recommendation on her site for one technology over the rest.

Some other academics, whom we did not study in class, like Peter Neumann who moderates the RISKS mailing list, are less optimistic. They agree mostly with the Caltech/MIT committee, but their papers focus on the immensity of the problem one faces when trying to design and implement a truly secure voting system. They often remind us of Ken Thompson's Turing acceptance speech and the fact that we really can't trust any code which we did not create ourselves. (And in reality, we cannot trust even code that we do write ourselves, since we almost always need a development toolchain written by someone else.) Therefore, they tend to be extremely suspicious of proprietary voting machines and their makers who insist that we should "just trust [them]."

Neumann [4] gives a list of suggestions for "generic voting criteria" which suggests that a

voting system should be so hard to tamper with and so resistant to failure that no commercial system is likely to ever meet the requirements, and developing a suitable custom system would be extremely difficult and prohibitively expensive.

Rebecca Mercuri [3,7] invented the "Mercuri method" for electronic voting. A critical component of this method is very similar to the Caltech/MIT proposal: a voting machine must produce human-readable hardcopy paper results, which can be verified by the voter before the vote is cast, and manually recounted later if necessary. Her philosophy and Neumann's are very similar; in fact, they've written papers together on the subject.

David Chaum presents a very interesting scheme [5], whereby voters could get receipts for their votes. This receipt would allow them to know if their votes were included in the final tally or not, and to prove *that* they voted without revealing any information about *how* they voted. The security of this scheme depends on visual cryptography developed by Naor and Shamir, and on voters randomly choosing one of two pieces of paper. Mercuri and Neumann advocate the use of this technique in electronic voting systems.

Dr. Michael Shamos of CMU provides a sharp counterpoint [6] to Neumann and Mercuri's views. While his "Six Commandments" summary of requirements for a voting system is very similar to others' requirements, he's less afraid of the catastrophic failures and sweeping fraud made possible by imperfections in electronic voting machines actually occurring in a real election. Shamos is also much less impressed with paper ballots than are Neumann and Mercuri. He places a great deal of faith in decentralization to make fraud difficult to commit and easy to detect. Dr. Shamos even *likes* DRE machines. (We must take into account the fact that this paper was written ten years ago, long before the 2000 elections and before more modern mathematical results like Chaum's; some of Dr. Shamos' opinions may have changed since then. While Dr. Neumann's talk cited here is of similar age, his pessimism with regard to machines has had little reason for change.)

Sources:

[1] "A Preliminary Assessment of the Reliability of Existing Voting Equipment," The Caltech-MIT Voting Technology Project, March 30, 2001 (revised).
Available at http://www.vote.caltech.edu/Reports/index.html)

[2] “Lorrie Cranor's Voting Papers,” Lorrie Faith Cranor.
http://lorrie.cranor.org/pubs/voting.html

[3] "A Better Ballot Box?" Rebecca Mercuri, IEEE Spectrum, Volume 39, Number 10, October 2002.

[4] “Security Criteria for Electronic Voting,” Peter Neumann, presented at the 16th National Computer Security Conference Baltimore, Maryland, September 20-23, 1993.
Available at http://www.csl.sri.com/users/neumann/ncs93.html

[5] “Secret-Ballot Receipts and Transparent Integrity,” David Chaum, draft.
Available at http://www.vreceipt.com/article.pdf

[6] “Electronic Voting - Evaluating the Threat,” Michael Ian Shamos, CFP '93.
Available at http://www.cpsr.org/conferences/cfp93/shamos.html\

[7] “Electronic Voting,” Rebecca Mercuri. http://www.notablesoftware.com/evote.html