Electronic Voting

Ronald L. Rivest

Laboratory for Computer Science
Massachusetts Institute of Technology
Cambridge, MA 02139
rivest@mit.edu

1 Introduction

Over the years, with varying degrees of success, inventors have repeatedly tried to adapt the latest technology to the cause of improved voting.

For example, on June 1, 1869 Thomas A. Edison received U.S. Patent 90,646 for an "Electric Vote-Recorder" intended for use in Congress. It was never adopted because it was allegedly "too fast" for the members of Congress.

Yet it is clear that we have not reached perfection in voting technology, as evidenced by Florida's "butterfly ballots" and "dimpled chads."

Stimulated by Florida's election problems, the California Institute of Technology and MIT have begun a joint study of voting technologies [5], with the dual objectives of analyzing technologies currently in use and suggesting improvements. This study, funded by the Carnegie Foundation, complements the Carter/Ford commision [6], which is focusing on political rather than technological issues. Electronic voting will be studied.

Among people considering electronic voting systems for the first time, the following two questions seem to be the most common:

Could I get a receipt telling me how I voted?

Could the U.S. Presidential elections be held on the Internet?

The first question is perhaps most easily answered (in the negative), by pointing out that receipts would enable vote-buying and voter coercion: party X would pay $20 to every voter that could show a receipt of having voted for party X's candidate. Designated-verifier receipts, however, where the voter is the only designated verifier—that is, the only one who can authenticate the receipt as valid—would provide an interesting alternative approach to receipts that avoids the vote-buying and coercion problem. See [4] for a discussion of this idea.

The second question—can we vote remotely over the Internet– is more problematic.

We start by noting that "electronic voting" includes a wide range of possible implementations. The California Internet Voting Task Force [1] distinguished between (a) voting at a supervised poll-site using electronic equipment, (b) voting at an unsupervised electronic kiosk (say, in a shopping mall), and (c) "remote voting"— voting from home or business using the voter's equipment.

Before proceeding to comment on the security of electronic voting systems, we should at least pause to consider the desirability of such systems. Is remote electronic voting over the Internet desirable? Why bother?

"Because we can" and "for increased voter convenience" are arguably insufficient justifications for electronic voting. "For increased confidence in the result" might be acceptable, if a convincing case could be made. Political scientists claim that the best justification is "to increase voter turnout."

In the remainder of this note, I discuss the "secure platform problem" as a key impediment to remote voting, and then provide a list of personal opinions regarding the security of electronic voting systems.

2 The "Secure Platform Problem"

There is a fundamental problem we must face when trying to design remote electronic voting systems: the "secure platform problem."

Cryptography is not the problem. Indeed, many wonderful cryptographic voting protocols have been proposed; see [2] for a sample bibliography.

The problem is interfacing the voter to the cryptography.

Almost all proposed cryptographic voting protocols *assume* that a voter (e.g. Alice) has a secure computing platform that will faithfully execute her portion of the protocol. The platform (e.g. a PC) will correctly display to Alice her intended vote, and cryptographically submit her vote during the protocol. The platform acts as Alice's "trusted agent" during the voting protocol.

In essence, the platform is *Alice as far as the voting protocol is concerned.*

In reality, the current generation of personal computers running Windows or Unix are not sufficiently secure to act as trusted voting agents. These operating systems and their applications are far too vulnerable to viruses and Trojan horses. A hacker could easily write a virus that would cause Alice's computer to display her voting for one candidate while actually voting for another. If thousands of PC's are similarly infected, an election could be rigged. This is an unacceptable risk.

Other studies and reports have reached similar conclusions that current technology is not secure enough to support electronic voting from home. In particular, I note the report of the California Task Force on Electronic Voting [1], Avi Rubin's note [7], and the Internet Policy Institute Report on Internet Voting[3].

Of course, the secure platform problem is not the only significant security problem that needs to be addressed regarding the possibility of electronic voting from home over the Internet. The Internet itself, while remarkably useful and reasonably robust, is all too vulnerable to flooding and denial of service attacks. The possibility that a foreign power could bring down the Internet on U.S. election day is all too real. For this reason alone, remote electronic voting from home over the Internet would be at best an available alternative, and it would be reasonable to expect existing poll-site voting systems to be prepared to handle everyone should the Internet be taken down.

3 Some personal opinions

3.1 E-Voting is not like E-Commerce

Electronic voting is unlike electronic commerce in several important ways, so it is insufficient to argue that secure electronic voting is merely a corollary to secure electronic commerce and that the same security mechanisms should apply.

For example, in electronic commerce there is always time to dispute a transaction if something hasn't worked correctly. With voting, there is a deadline that must be met.

Also, in an electronic commerce transaction, the buyer typically gets a receipt that can be used later to resolve disputes. In contrast, it is important, as noted earlier, that voters do *not* get receipts showing how they voted, since this may enable the voter to sell his vote.

In electronic commerce, transaction records identify the parties involved. In electronic voting, the ballots cast should *not* identify the voters who cast them, as this might violate the voter's privacy and subject them to coercion. (For example, if election officials could see how each voter voted, then the lead election official could see how his employees voted.)

3.2 It is more important that no one "has their thumb on the scale" than having a scale that is easy to use or even very accurate.

The primary purpose of a voting system is to correctly determine the will of the voters. Given human nature, the likelihood of getting an incorrect result is much higher if there are significant security vulnerabilities than if the vote-counting is a bit inaccurate. Fraud can be a problem in any election; counting errors affect only close elections. Ease of use is relevant only inasmuch as it affects voter turnout or introduces systematic biases.

Electronic voting from home runs the risk of allowing an adversary to put a "big thumb" on the scale, since the adversary may be able to automate his attack. For example, he could bring down the Internet in Democratic neighborhoods, or create a virus that affects computers with certain characteristics (e.g. those with ".edu" suffix). Such risks threaten the primary purpose of the voting system, and suggest exceptional caution in moving forward with such systems.

3.3 The voting system must be simple to understand and operate. Electronic voting systems are often complex.

Voting systems must be certified before they are used. Election officials must have confidence that the voting system will prevent fraud and perform reliably.

Complexity is the enemy of security. Complex systems are difficult to understand and debug. Asking an election official to certify that thousands of lines of code provide a secure and trust-worthy election system is an entirely different matter than asking him to certify a set of procedures for managing a collection of paper ballots. Electronic voting systems place a substantial burden on the

election officials who must certify the systems, and may weaken the credibility of the entire process in the voters' minds.

Even with poll-site electronic voting, the complexity of electronic voting systems may also challenge the election officials (who are often volunteers) who must install and operate the election equipment. The failure to educate both election officials and voters to use new equipment properly is a major source of election problems.

3.4 Physical ballots can provide better audit trails than purely electronic systems.

The integrity and trust-worthiness of a voting system is greatly enhanced by having an audit trail recording each ballot cast. Many states require voting systems to have such audit trails.

Audit trails with very high integrity can be obtained when the audit trail is created directly by the voter, as with a paper ballot. Electronic voting systems are *indirect*—they interpose a layer of mechanism between the voter and the audit trail, risking the possibility that the mechanism is not faithfully capturing the voter's preferences.

Nonetheless, paper ballots are not perfect either, and Shamos [9] gives interesting arguments in favor of electronic audit trails. Saltman's classic work [8] discusses in some detail audit-trail requirements for electronic voting systems.

3.5 County-level decisions on voting technology has benefits.

There are clear and probably compelling advantages to specifying and purchasing voting systems on a state-wide basis rather than county by county, as is currently the case in the U.S. But we should not lose sight of two arguments to the contrary.

First, just as a woodland's diverse variety of plants can provide better resistance to pathogens than the farmer's single crop, so too can a variety of voting technologies provide resistance to an adversary's attack, as there is no common point of vulnerability for the whole system.

Second, we need ways to gain experience with new voting systems. One good way is to allow individual counties to experiment with techniques that are different than the state-wide norms.

3.6 The ability to handle disabled voters will become increasingly important.

Existing voting systems tend to be poor at accommodating the needs of disabled voters. For example, blind voters have had to trust election officials to read the ballots and enter their votes. Electronic voting systems are capable of supporting a diversity of interfaces to the voter.

3.7 Our largest security problem is likely to be *absentee ballots*.

Absentee voting has increased dramatically over the past decade. Indeed, some states, such as Oregon, vote entirely by mail. Remote electronic voting can be viewed as a version of absentee voting.

In my opinion, however, by allowing such an increase in absentee voting we have sacrificed too much security for the sake of voter convenience. While voters should certainly be allowed to vote by absentee ballot in cases of need, allowing voting by absentee ballot merely for convenience seems wrong-headed. I would prefer seeing "Voting Day" instituted as a national holiday to seeing the widespread adoption of unsupervised absentee or remote electronic voting.

4 Summary

Some paper-based voting technologies, such as optical scanning, offer reasonable balances of security, ease of use, cost, simplicity, and reliability. (Other paper-based technologies, such as punch cards, should definitely be phased out.)

Electronic voting systems promise benefits in terms of ease of use, especially for disabled voters. Because of the software-based and indirect character of electronic voting systems, these benefits come at the cost of increased complexity and at the risk of decreased security.

While electronic voting from home should perhaps forever remain too risky a fantasy, electronic poll-site voting may provide, even in the near term, worthwhile improvements to paper-based voting technologies. Cryptographic techniques will certainly be essential in any electronic voting technology, as will better methods for addressing the "secure platform problem."

References

1. California Internet Voting Task Force. Final report. Available at `http://www.ss.ca.gov/executive/ivote/`.
2. Rachel Greenstadt. Electronic voting bibliography, January 2000. Available at `http://theory.lcs.mit.edu/ cis/voting/greenstadt-voting-bibliography.html`.
3. Internet Policy Institute. Internet voting. Available at `http://www.internetpolicy.org`.
4. M. Jakobsson, K. Sako, and R. Impagliazzo. Designated verifier proofs and their applications. In Ueli Maurer, editor, *Advances in Cryptology - EuroCrypt '96*, pages 143–154, Berlin, 1996. Springer-Verlag. Lecture Notes in Computer Science Volume 1070.
5. California Institute of Technology and Massachusetts Institute of Technology. Voting technology project. `http://www.vote.caltech.edu/`.
6. National Commission on Federal Election Reform. Available at `http://www.reformelections.org`.
7. Avi Rubin. Security considerations for remote electronic voting over the internet, 2000. Available at `http://avirubin.com/e-voting.security.pdf`.

8. Roy G. Saltman. Accuracy, integrity, and security in computerized vote-tallying. Technical report, Computer Science and Technology, National Bureau of Standards, Gaithersburg, MD 20899, August 1988. NBS Special Publication 500-158. Available at `http://www.itl.nist.gov/lab/specpubs/500-158.htm`.
9. Michael Shamos. Electronic voting—evaluating the threat. Presented at CFP '93. Available at `http://www.cpsr.org/conferences/cfp93/shamos.html`.