electronic voting

Main

a form of computer-mediated voting in which voters make their selections with the aid of a computer. The voter usually chooses with the aid of a touch-screen display, although audio interfaces can be made available for voters with visual disabilities. To understand electronic voting, it is convenient to consider four basic steps in an election process: ballot composition, in which voters make choices; ballot casting, in which voters submit their ballots; ballot recording, in which a system records the submitted ballots; and tabulation, in which votes are counted. Ballot casting, recording, and tabulation are routinely done with computers even in voting systems that are not, strictly speaking, electronic. Electronic voting in the strict sense is a system where the first step, ballot composition (or choosing), is done with the aid of a computer.

There are two quite different types of electronic voting technologies: those that use the **Internet** (I-voting) and those that do not (e-voting). These two types are described in this article.

I-voting

As use of the Internet spread rapidly in the 1990s and early 21st century, it seemed that the voting process would naturally migrate there. In this scenario, voters would cast their choices from any computer connected to the Internet—including from their home. This type of voting mechanism is sometimes referred to as I-voting. Beyond voting in regularly scheduled elections, many saw in the emergence of these new technologies an opportunity to transform democracy, enabling citizens to participate directly in the decision-making process. However, many countries decided that the Internet was not secure enough for voting purposes. Limited I-voting trials have been undertaken in some countries, including Estonia, Switzerland, France, and the Philippines. The case of **Estonia** is especially enlightening: although the country's infrastructure for digital democracy is highly developed, use of the Internet has been at times massively disrupted by **denial-of-service attacks**. This has forced the country to maintain its traditional voting infrastructure alongside the I-voting option.

Besides denial-of-service attacks on the Internet, security experts worry that many **personal computers** are vulnerable to penetration by various types of malware (malignant software). Such attacks can be used to block or substitute legitimate votes, thereby subverting the electoral process in a possibly undetected way.

A third concern about I-voting relates to the possibility of voter coercion and vote selling, which in principle can more easily occur when voting does not take place in a controlled environment. However, there is no consensus about the seriousness of this problem in stable democracies. Furthermore, this objection also applies to absentee ballots, which have been broadly used in the past, as well as vote-by-mail.

E-voting

Because of security and access concerns, most large-scale electronic voting is currently held in designated precincts using special-purpose machines. This type of voting mechanism is referred to as e-voting. There are two major types of e-voting equipment: direct recording electronic (DRE) machines and optical scanning machines.

A typical DRE is composed of a touch screen connected to a computer. Ballots are presented to the voters on the touch screen, where they make their choices and cast their ballot. The touch-screen display can be used to assist the voter in a variety of ways, which include displaying large fonts and high contrast for those with limited vision, alerting the voter to undervotes, and preventing overvotes.

A DRE directly records the cast ballots and stores the data in its memory. Thus, a single machine is used for composition, casting, and recording of votes. The third step, recording of the cast ballot in a memory device, is invisible to the voter. Assurance that the vote is recorded as cast relies on testing of the machine's hardware and software before the election and confidence that the software running during the election is the same software as the one tested before the election. Both of these are subjects of much controversy.

Whereas testing for faults in hardware or unintentional errors in software can be highly reliable, the same is not true for malicious software. Most security professionals believe that an insider attack at the software development stage could make it to the final product without being detected (although there is disagreement about the likelihood of such an attack). This problem is compounded by the fact that **source code** is usually not made available for public scrutiny.

Computer viruses can infect a machine during an election. For this to happen, the machine must somehow interact with another **electronic device**. Thus, connection to the Internet or to wireless devices is usually disallowed. However, a voting session is typically initiated through the use of an activation card. A poll worker, upon verification of eligibility, sets the card to enable one voting session. After the session the voter returns the card to the poll worker for reuse. At least one DRE system has been shown to be vulnerable to infection using the activation card. An infected machine can be made to record votes not as they were cast.

The threat of DREs not recording the votes as cast has led some individuals and organizations to argue that a paper audit record must be produced for each cast ballot. DRE manufacturers responded by adding a printer capability to their DREs. The resulting systems produce both an electronic record and a paper record. However, problems in handling and monitoring the paper record, both by voters and by election officials, have led to much criticism of these hybrid systems. Many jurisdictions have discarded them in favour of optical scanning technology.

In some **optical scanning** systems the voter fills out a paper ballot and inserts it into an electronic scanning device. Scanners can reject improperly marked ballots, allowing the voter to start over, thereby reducing discarded votes.

In other optical scanning systems voters compose their votes on a computer screen. Once a ballot is completed, the computer prints an optical scanning ballot. The voter verifies the ballot and then inserts it in another device that scans and tabulates the vote. Both these systems are considered electronic voting systems.

None of the above electronic voting systems is completely secure. Opinions differ widely on whether the posited threats are realistic enough to warrant forgoing the added functionalities of electronic voting in favour of the perceived security of nonelectronic voting systems. Cryptographers, on the other hand, have devised systems that allow voters to verify that their votes are counted as cast. Additionally, these systems do not enable the voter to prove to a **third party** how they voted (thus reducing the risks of vote selling and coercion). These cryptographic systems, called end-to-end (E2E) secure, are the preferred systems from a security point of view. Thus, there is considerable academic interest in fully developing these systems. On the other hand, some people argue against E2E systems on the grounds that their mathematical underpinnings are not comprehensible to the average voter.

René Peralta

Additional Reading

R. Michael Alvarez and Thad E. Hall, *Point, Click, and Vote: The Future of Internet Voting* (2004), discusses issues related to using the Internet for voting. Donald G. Saari, *Chaotic Elections! A Mathematician Looks at Voting* (2001), examines the many ways to democratically pick a winner and the provable fact that no way is perfect. Dimitris Gritzalis (ed.), *Secure Electronic Voting* (2002), is a collection of academic papers on the subject. United States Election Assistance Commission, *Voluntary Voting System Guidelines* (2005), contains a set of specifications and requirements against which voting systems can be tested in the United States. These guidelines are undergoing major revisions; there is a draft under consideration at http://www.eac.gov.

Citations

MLA Style:

"**electronic voting**." Encyclopædia Britannica. 2009. Encyclopædia Britannica Online. 10 Apr. 2009 <**http://www.britannica.com/EBchecked/topic/1472946/electronic-voting**>.

APA Style:

electronic voting. (2009). In *Encyclopædia Britannica*. Retrieved April 10, 2009, from Encyclopædia Britannica Online: **http://www.britannica.com/EBchecked/topic/1472946/electronic-voting**