Electronic voting has been proposed in a number of precincts in the USA. One of the most extensive archives of discussions about this issue is the RISKS FORUM DIGEST edited by Peter G. Neumann of SRI Intl. Entering “vote” as a keyword in the search engine available through at <http://catless.ncl.ac.uk/Risks/> brings up 303 entries starting with Volume 1 Number 1 [henceforth notated as “v(n)” for the volume and number] in 1985; additional articles can be found using other related keywords such as “voting” and “election.”

One of the most recent contributions comes from Jonathan Kamens, writing in RISKS 22(39) (23 Nov 2002). He describes a system that allows a voter to mark a paper ballot and then feed it in through an electronic reader. Kamens points out that the card-reading voting system proposed for Boston MA has fundamental problems:

* There is no way for a voter to verify that the system is correctly registering the voter's choices on the ballot.

* If the card reader indicates that a card has not successfully been registered, a voter can be given a second card -- but the invalid one goes straight into a locked ballot box. If there's a recount, someone could get both their ballots counted.

In general, e-voting systems can include any or all of the following functions, each requiring increasing degrees of security:

* Automatic reading and tallying of votes made on paper ballots;

* Accepting votes using electronic input devices such as electric pens, touch-screens, and keyboards;

* Remote voting at a distance.

E-voting systems need to include at least the following security characteristics:

1) Remote voting requires identification, authentication and authorization PLUS guarantees of complete privacy as well as measures to prevent fraudulent exclusion of valid voters and fraudulent acceptance of repeated votes by individuals.

2) Electronic data entry should include all the measures developed in the last 40 years of data processing to reduce the likelihood of user error; such measures include

a) feedback to the user to be sure that what was entered was what was recorded;

b) error checking and alerts to prevent obvious blunders such as voting for two people for the
same position if that is not permitted;

c) provision of overrides so that voters can deliberately spoil their ballot if that's what they want to do;

3) Fail-safe redundancy so that no single point of failure or even widespread denial-of-service attacks could wipe out voter's intentions;

4) Cryptographically strong local and remote audit trails to keep multiple independent records of all votes; such files could include checksums that are calculated using the preceding record's checksum as input to the hashing algorithm (to reduce the ease of fraudulent tampering with the records).

One of the most serious questions raised about e-voting is independent of security: it’s the issue of equal access. Will widespread e-voting lead to increased disparity between the voting patterns of richer and poorer people among the electorate? Will e-voting be yet another example of what has been called the “digital divide?”

* * *

In the next article in this two-part sequence, I will look at some detailed analyses of e-voting with special attention to security.

* * *

For further reading:


Digital Divide Network <http://www.digitaldividenetwork.org/content/sections/index.cfm>


Electronic Frontier Foundation “E-voting” Archive <http://www.eff.org/Activism/E-voting/>

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.
