Vermont has a tiny population; we have about 600,000 people in the entire state. Because of this small population, people here have many ways of becoming involved in civic affairs. Our state house in Montpelier (the smallest state capital city in the US, with 8,000 people) is open to the public, as are committee meetings. State officials such as the governor often walk about in town where ordinary citizens can chat with them in a friendly and very personal way.

I was recently invited to address the Government Operations Committee as they discussed a pending bill which would require any wholly electronic voting mechanism to be equipped with a means of producing a paper ballot that could be inspected by the voter and which would then be stored safely for official recounts. Given the importance of safeguarding the vote in our nation, I thought it might interest readers to step outside the confines of network security for a moment to consider the security implications of wholly electronic voting.

Today, there are three different forms of voting in place in use in the USA (I won’t discuss remote, Internet-based voting in this column): one can mark a piece of paper by hand and have it read by people; one can mark a piece of paper by hand or machine and have it read by an optical-mark reader which tallies the results automatically; or one can use a wholly-electronic system with an input device such as a touch-sensitive screen which stores the results in a database and produces automatic tallies.

Normally, paper ballots, whether read by people or tallied by machines, are stored in sealed containers and can be opened with a court order in cases of judicially-approved recounts when election results are challenged.

In Vermont, the Secretary of State’s office allows optical-mark readers to be used for elections; only one such machine is required per voting location, most of which have at most a few thousand voters registered per location. However, most locations still use manual counting of ballots under the supervision of representatives of the various political parties involved in the election.

In my testimony before the Government Operations Committee, I stressed the following points:

* Any system of vote counting that relies on completely proprietary (secret) programs is potentially vulnerable to abuse. The underlying computer programs controlling how marks on ballots are counted in Vermont are proprietary (they are owned by Diebold Corporation), but the technicians who prepare the configuration tables relating a position on a ballot to a particular name work for an independent consultancy in Massachusetts and their configuration tables are open for inspection.

* Every optical tabulator is tested to see if it reads ballots correctly before the election begins.

* Passing a law that allows the Secretary of State to order a random check on the accuracy of machine tallies in any voting district will help prevent systematic fraud. The tallies in a manual
recount must match the machine tallies to within an acceptable error rate (to allow for the inherent difference between machine tallies and human counting methods: machine reject incorrectly-marked ballots whereas people can agree on the intention of the voter).

* Wholly-computer-based voting systems have far more vulnerabilities to tampering than optical-mark sensors. We know that even companies such as Microsoft have allowed Easter Eggs (unauthorized, undocumented code such as flight simulators) to escape quality assurance and be delivered to customers in software such as MS-Excel. We know that microprocessors have been tampered with to cheat clients and evade testing (e.g., gas pump meters in the Los Angeles district were designed to overcharge customers by 10% -- unless they noticed one- or five-gallon deliveries, which were the volumes typically used by inspectors when checking accuracy). We know that production code has been profoundly flawed for years without being caught (e.g., the Colorado lottery’s not-very-random-number generator that produced only numbers from zero to eight but never any nines). We know that data stored in databases without careful attention to chained cryptographic checksums involving timestamps, sequence numbers and the previous record’s checksum can be modified to misrepresent election results.

* For all these reasons, we should resist the use of wholly-computerized voting machines until there is software that is entirely open to inspection.

* Any wholly-electronic voting machine should be required to produce a paper ballot showing the voter’s choices for inspection by that voter (only). The voter should then be required to place the ballot in a ballot box for use in judicial recounts and random testing of the accuracy of the computerized voting system.

* * *

For further reading:

Background paper on all aspects of electronic voting < http://lorrie.cranor.org/voting/hotlist.html >


Dangers of proprietary code in voting machines < http://www.blackboxvoting.org >

See also several articles and press releases about electronic voting on the Electronic Frontier Foundation Web site at < http://www.eff.org >


* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Copyright © 2004 M. E. Kabay. All rights reserved.
Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.