Guest Opinion

An urgent need for 'open-source' voting systems

by Arthur Keller

The principle of voting in the United States is that votes are cast in secret but tallied in public.

This principle is incompatible with the current practice of using voting systems whose inner workings are trade secrets owned by the voting-machine vendors. Those same vendors pay for their systems to be tested, and the results of those tests are also trade secrets — you guessed it — owned by the vendors.

Something is terribly and urgently wrong.

The usual claims for secrecy are that it somehow enhances security. The evidence for security through obscurity in software is quite limited. Some argue that the Apache web server, the software that powers 60 percent of the world's Web sites, compares favorably to Microsoft's Web server because the Apache source code is publicly available.

Although Microsoft does not publicly release its Web server's source code, Microsoft will make the source code†available to large customers under license. In contrast, the source code of voting systems is not available for inspection even by counties that purchase these systems and certainly not for inspection by you or me.

We're all familiar with how the excuse of military security is often used to cover up embarrassing information that has little security value. Why wouldn't vendors use trade secrets as an excuse to cover up flaws in their systems or merely shoddy workmanship? In fact, the exposed Diebold e-voting source code has shown embarrassing details.

We do not know what lurks in the programming of the other vendors. Fortunately, ES&S and Sequoia have promised San Francisco and Alameda counties that they will cooperate with source code disclosure rules if the state requires it. Unfortunately, the current California secretary of state opposes such disclosure rules. The Open Voting Consortium (www.openvoting.org) is creating a registry where vendors can publish voting systems technology. This registry will include requirements for what must be disclosed, such as software source code, specifications, documentation and hardware designs. While vendors may retain proprietary rights to the software, vendors must allow testing, experimentation, analyses and publication by anyone.

While anyone will be allowed to inspect the software, of course not everyone has the skills to do so effectively. But individuals or groups will be able to hire the expert of their own choosing and to publish their analyses. Today the only experts allowed are those chosen by the vendors themselves or by election officials, and their analyses are usually kept secret, and when released, are heavily redacted (censored).

This secrecy makes voting systems vulnerable to inaccuracy, or worse, fraud. In turn, voters lose confidence that their votes are counted as cast and cast as they intended.

The Help America Vote Act (HAVA) was enacted in 2002 in the aftermath of the 2000 Presidential election, when it became clear that our current voting systems were inconsistent, unreliable and unfair. However, the post-HAVA federal standards were not created until late 2005, and these are voluntary and do not require paper ballots or paper trails, auditing or adequate testing.

No wonder most computer scientists have grave concerns about existing voting systems.

Are the newly purchased systems that we'll use on Nov. 7 also inconsistent, unreliable and unfair? We just don't know.

While some claim that there is a risk in publishing software developed in secret and not designed to be published, continued secrecy is not the solution. Rather, the solution is replacement of secret software too fragile or embarrassing to publish with a more robust, open-source voting system, where anyone can inspect the software.

Just as the security of Apache is enhanced by its publication, the publication of an open-source voting system will help ensure that the system is secure and reliable.

It is a myth that anyone can make changes to open-source software such as Apache. Certainly anyone can download Apache, make changes to it and run the changed version. But changing the official version of Apache can be done only by a small number of people in a carefully controlled process.

Anyone can report a bug in Apache or a suggested improvement. But any suggested improvement will go through levels of analysis and scrutiny before it is adopted. And that scrutiny is far higher than voting-system vendors, testers or inspectors can muster.

In a variety of industries, the government has sponsored research and development work that has produced systems later adopted by industry. Military-funded research leads to the creation of products and services that the military can buy. It is time for the government to fund the creation of an open-source voting system that vendors can adopt to provide more choices to election officials to buy on behalf of the voters.

Open-source voting systems will mean additional choices available not only for the initial procurement of voting systems but also for ongoing maintenance and support, and for auditing and reporting systems.

It is reported that years ago an IBM salesman said to a prospective customer, "Be careful not to get locked into open systems." But now IBM is one of the biggest proponents of open systems.

It is time for our election officials to become proponents of open systems, too — and for the public to demand them. ■

Arthur Keller is a founder and board secretary of the Open Voting Consortium and a precinct inspector in Santa Clara County. He can be e-mailed at arthur@openvoting.org.