



COTS and Other Electronic Voting Backdoors

During the U.S. 2006 primary election season, there was a flurry of media attention about electronic voting, when it was revealed that Diebold Election Systems had erroneously reported to a testing authority (CIBER) that certain Windows CE operating system files were commercial-off-the-shelf (COTS) but in fact also contained customized code. This is important because, remarkably, all versions of the federal voting system guidelines exempt COTS hardware and software from inspection, whereas modified components require additional scrutiny.

This loophole is anathema to security and integrity. In other critical computer-based devices (such as medical electronics or aviation), COTS components may be unit-tested once for use in multiple products, with COTS software typically integration-tested and its source code required for review. In contrast, for voting equipment, this blanket inspection exemption persists, despite having strenuously been protested by numerous scientists, especially in the construction of guidelines authorized by the Help America Vote Act (HAVA). Nevertheless, special interests have prevailed in perpetuating this serious backdoor in the advisory documents used for U.S. voting system testing and certification programs.

Indeed, Diebold dismissed the discovered customizations as presenting only “a theoretical security vulnerability that could potentially allow unauthorized software to be loaded onto the system”; a Diebold spokesman commented “for there to be a problem here, you’re basically assuming ... you have some evil and nefarious election officials who would sneak in and introduce a piece of software. ... I don’t believe these evil elections people exist.” But such naiveté is laughable, as there is a long and well-documented history of such “political machines” and operatives in the U.S.

Uninspected COTS has caused other serious voting equipment problems to go undetected, even if tampering is not an issue, as reported in 2001 to the U.S. House Science Committee by Douglas Jones, when he related a 1998 example of “an interesting and obscure failing [with the Fiddler and Chambers EV 2000] that was directly due to a combination of this exemption and a recent upgrade to the version of Windows being used by the vendor ... the machine always subtly but reliably revealed the previous voter’s vote to the next voter.”

The strong resistance to closing this COTS backdoor was illustrated by the activities of the IEEE’s P1583 Voting System Standards working group, while they were drafting a document to be submitted as input to the Election Assistance Commission’s (EAC) Technical Guidelines Development Committee. A Special Task Group (STG) was formed to resolve COTS-related issues in the draft. Although all issues were resolved with strong consent by the STG’s members, P1583’s vendor-partisan editing committee unabashedly repeatedly refused to incorporate any of the substantial COTS review requirements into the draft. Therefore, the version of the document released to the EAC still contained the exemption for COTS components, even though the working group had decided otherwise.

Numerous other aspects of U.S. voting equipment certification process are similarly lax. Another P1583 working group member, Stanley Klein, repeatedly pointed out to the EAC that the legacy low 163-hour Mean Time Between Failures rate specified in all versions of the voting system guidelines translated to an Election Day malfunction probability (potentially resulting in unrecoverable loss of votes) of 9.2% per machine, to no avail. Attempts to require a Common Criteria style evaluation were frustrated. Bizarrely, the guidelines allow for the risky use of wireless transceivers in voting machines, but do not require that the ballot data be provided in a format such that it is independently auditable. And although there is a federal certification process, there is no provision for decertification, even when a major security flaw has been exposed. The fact that any changes, including security-related ones, require recertification, has even been used as an excuse to avoid making needed updates. Indeed, the nature of U.S. elections is such that federal certification, as poor as it is, is not mandatory; one-fifth of the states have chosen to disregard it, some in lieu of even more haphazard and obfuscated examination processes.

This distressing situation will likely continue until large numbers of citizens, especially those with technical expertise, hold government officials accountable. You can help by communicating with your elected officials, beseeching them to do something about this now. **■**

REBECCA MERCURI (mercuri@acm.org) is a forensic computing expert who has been researching electronic voting since 1989. **VINCENT LIPSIO** (vince@lipsio.com) is a software engineer who specializes in real-time and life-critical systems. **BETH FEEHAN** (bfeehan@comcast.net) is a researcher focusing on HAVA implementation issues.