Consumer organisation highlights security hole in US vote-counting system

Mike Ingram
10 September 2004

Black Box Voting, a non-profit organisation that specialises in exposing possible electoral abuses, has published details of a security hole in America's Diebold GEMS central vote tabulator. The security hole has been know about for a year with no action being taken to rectify the problem.

According to blackboxvoting.org: "By entering a 2-digit code in a hidden location, a second set of votes is created. This set of votes can be changed, so that it no longer matches the correct votes. The voting system will then read the totals from the bogus vote set. It takes only seconds to change the votes, and to date not a single location in the US has implemented security measures to fully mitigate the risks."

Pointing out that the programme was designed and tested over a series of a dozen version releases, the site states that the flaws cannot be put down to "stupidity or sloppiness". The founder of Blackbox Voting, Bev Harris, concludes: "The GEMS central tabulator program is incorrectly designed and highly vulnerable to fraud. Election results can be changed in a matter of seconds. Part of the program we examined appears to be designed with election tampering in mind. We have also learned that election officials maintain inadequate controls over access to the central tabulator."

The weaknesses in the system were first published in July 2003 and have since been corroborated by independent studies, and Diebold's own internal memos written by programmers who have worked on the system. Harris says that despite this, "Not a single location has yet implemented the security measures needed to mitigate the risk."

The California Attorney General was made aware of the problem nearly a year ago, but no action has been taken. "Rather, Gov. Arnold Schwarzenegger recently froze the funds, allocated by Secretary of State Kevin Shelley, which would have paid for increased scrutiny of the voting system in California," Harris says.

The site catalogues a series of incidents going back to November last year which show a systematic refusal to address the problem:

* November 2003: Harris and Black Box Voting director Jim March "filed a Qui Tam lawsuit in California citing fraudulent claims by Diebold, seeking restitution for the taxpayer. Diebold claimed its voting system was secure. It is, in fact, highly vulnerable to and appears to be designed for fraud."

* February 2004: Black Box Voting Associate Director Andy Stephenson and Harris visited the Washington Attorney's office to inform them about the problem.

* April 21, 2004: Harris appeared before the California Voting Systems Panel, and presented a document showing that Diebold had not corrected the GEMS flaws, even though it had updated and upgraded the GEMS program.

* August 8, 2004, Harris demonstrated to the leading Democrat Howard Dean how easy it is to change votes in GEMS, on CNBC TV.

*August 11, 2004: Jim March formally requested that the California Voting Systems Panel watch the demonstration of the double set of books in GEMS. They were already convened, and the time for Harris was already allotted. Though the demonstration takes only three minutes, the panel refused to allow it and would not look. "They did, however, meet privately with Diebold afterwards, without informing the public or issuing any report of what transpired," Harris says.

* August 18, 2004: Harris and Stephenson, together with computer security expert Dr. Hugh Thompson, and former King County Elections Supervisor Julie Anne Kempf, met with members of the California

Voting Systems Panel and the California Secretary of State's office to demonstrate the double set of books. The officials declined to allow a camera crew from "60 Minutes" to film the meeting.

According to Harris: "The Secretary of State's office halted the meeting, called in the general counsel for their office, and a defence attorney from the California Attorney General's office. They refused to allow Black Box Voting to videotape its own demonstration. They prohibited any audiotape and specified that no notes of the meeting could be requested in public records requests. The undersecretary of state, Mark Kyle, left the meeting early, and one voting panel member, John Mott Smith, appeared to sleep through the presentation."

Diebold cannot claim ignorance of the problem, as it issued a cease and desist notice on the *blackboxvoting.org* website when the security holes were first reported in 2003.

The systems in question are used to count votes in over 30 states, regardless of what method of voting is used—absentee, touch-screens, paper ballot or optical scan machines. Each of the 1,000 machines counts up to two million votes at once.

Harris says: "The central tabulator is far more vulnerable than the touch screen terminals. Think about it: If you were going to tamper with an election, would you rather tamper with 4,500 individual voting machines, or with just one machine, the central tabulator which receives votes from all the machines? Of course, the central tabulator is the most desirable target."

While election industry officials insist that the tabulator is secure because it is protected by passwords and audit logs, the author insists that GEMS passwords can easily be bypassed, and the audit logs can be altered and erased. "Worse, the votes can be changed without anyone knowing, including the officials who run the election," Harris says.

The software, which runs on a Microsoft Access database, breaches basic requirements of properly designed accounting software. Such applications prohibit the creation of two sets of books precisely because this is open to fraud. "Any properly designed accounting program will allow only one set of books. You can't enter your expense report in three different places. All data must be drawn from the same place, and multiple versions are never acceptable. But in the files we examined, we found that the GEMS system contained three sets of 'books'," Harris says.

Whereas accounting packages automatically link up data tables to each other to prevent back door entries, the GEMS system used by Diebold allows a two-digit code to be typed into a hidden location, with which the tables can be decoupled—allowing the voting system to draw information from a combination of real votes and a set of fake votes that can be altered at will. All of this cannot be seen by the elections official, who never sees the different set of books. All the official sees is the reports they can run, election summary, statements of votes cast, etc.

With the presidential elections less than two months away, it is remarkable that this issue has been paid so little attention by the US media. Given the events of November 2000 which saw the presidency handed to George W. Bush under circumstances in which thousands of votes in Florida remained uncounted, no one can discount the possibility that the electronic manipulation of the vote this time around is being actively considered.