
California: Integrity of E-Balloting System Still In Doubt

(February 23, 2006) - Contributed by Michael Hiltzik, Golden State

This editorial appeared in the Los Angeles Times on February 23, 2006. It is reposted here with permission of the author. Michael Hiltzik's contributes to the Golden State Blog.

Let's face it: When it comes to computer security, we're all slobs. At work, we scribble our secret passwords on our desk blotters. At home, we leave our Internet connections open to be peeked through by anyone — whether the neighbor next door or a geek in pajamas halfway around the world. We forget our laptops in taxicabs, and transmit our credit card numbers to strangers over the Web.

Generally, the consequences are trivial. Most of the information let loose into cyberspace is, frankly, of no interest to anybody. But there's no excuse for exposing the integrity of our election system to computer hackers. Yet that's what California Secretary of State Bruce McPherson may have done last week by approving electronic voting machines from Diebold Election Systems for use in California elections through the end of this year. McPherson's approval was conditioned in part on local election officials keeping the Diebold machines under tight security before polls open. Diebold will have to make significant changes to its software and undergo further scrutiny from state and federal authorities for 2007. Given the rising panic among county registrars about having machines ready for the June primary, it's hard to avoid the impression that McPherson's decision reflected expediency more than confidence in Diebold's work.

Indeed, his ruling produced a statewide sigh of relief from county registrars, who were squeezed between a federal law requiring them to install efficient new high-tech poll machines and a state law requiring the machines to be formally certified. "This means I won't have to go to either Leavenworth or Folsom," San Diego registrar Mikel Haas told me. His county, which will stage a primary on April 11 to replace the bribe-taking Rep. Randy "Duke" Cunningham, bought 10,200 Diebold machines for \$31 million in 2003, but hadn't been allowed to use them since 2004.

As the last two presidential elections demonstrate, ballot results are of profound interest to everybody — including determined hackers with partisan agendas. Therefore, it's proper to demand of the high-tech machines replacing the paper ballots and punch cards of yore that they be technologically bulletproof. The Diebold systems certified by McPherson — an optical scanner that reads hand-marked ballots and a touch screen that totes up votes directly — fall well short of that standard.

How do we know this? It's the conclusion of a panel of computer security experts McPherson commissioned specifically to study Diebold's software. Three days after they issued their report Feb. 14, McPherson gave Diebold thumbs up, noting that the panel regarded the software problems it found as "manageable" and had said the risks could be "mitigated" if election officials took care.

But the experts were plainly troubled by flaws in Diebold's systems. The panel, which included David Jefferson of Lawrence Livermore National Laboratory and David Wagner of Berkeley, observed that the removable memory cards used by Diebold were vulnerable to undetectable acts of tampering.

The panel found 16 software bugs that could cede "complete control" of the system to hackers who might then "change vote totals, modify reports, change the names of candidates, change the races being voted on," and even crash the machines, bringing an election to a halt. Hackers wouldn't need to know passwords or cryptographic keys, or have access to any other part of the system, to do their dirty work. Voters, candidates and election monitors wouldn't necessarily know they'd been rooked.

The bugs lead some computer professionals to believe that Diebold's software designers never treated security as a high priority. "It's like they were making a mechanical device, and never heard of computer security," says David Dill, an expert in electronic voting at Stanford University who wasn't on the panel.

The bugs pale next to another discovery by the panel. This is the presence of a cryptographic key written into the source code, or basic software, of every Diebold touch-screen machine in the country. The researchers called this blunder tantamount to "a bank using the same PIN code for every ATM card they issued; if this PIN code ever became known, the exposure could be tremendous."

Here's the punch line: The Diebold key became known in 2003, when it was published by researchers at Johns Hopkins and Rice universities. It can be found today via a Google search. What's worse, the key was first identified in 1997 by a University of Iowa researcher, who promptly warned the manufacturer of the flaw, apparently to no avail.

Diebold contended in 2003 that the Hopkins-Rice researchers had examined "an older version" of its code, suggesting that the flaw had been removed. But that doesn't explain why the same defect was found this year by the Berkeley panel,

which wrote that it was hard-pressed "to imagine any justification" for continuing to use a cryptographic key that had been publicly compromised.

A Diebold spokesman told me that the key isn't a security issue today because election officials are instructed to override it with their own key before running the machines. McPherson's office requires county officials to perform the override as a condition to allowing them to use the machines. But many computer security experts say that's a poor solution. The human factor is an inherent flaw in any security system, and it's a mistake to rely on overstressed and overworked election officials to run through a complicated checklist, especially when the procedure would be unnecessary if the system were designed properly in the first place.

The Berkeley panel says there may be other undetected flaws lurking in the Diebold software, which indicates that electronic voting isn't yet ready for Election Day. "We know we're going to have a loser in the next election, and that loser may not be convinced he or she has lost," says Avi Rubin, a Johns Hopkins professor who co-authored the 2003 paper. "We don't need to give people another reason to doubt an election."