

NEWLY DISCOVERED DIEBOLD THREAT DESCRIBED AS 'MAJOR NATIONAL SECURITY RISK!' 5/5/06

-- Voting Systems in Question Were Used Last Week in Ohio Primary, Soon in Pennsylvania
-- So 'Serious' Few Details Are Being Released. -- *All Diebold Touch-Screen Machines, In All States, Said to be Affected by 'Horrific' Vulnerability, Systems 'Sequestered' in PA*

An official Pennsylvania state warning has been issued about the new "security vulnerability" discovered in all Diebold touch-screen electronic voting machines.

That warning, which has now brought a lock-down on all Diebold systems in PA, where early absentee (non-machine) voting is about to begin prior to their upcoming May 16th primary election, was reported by the *Morning Call*¹ yesterday. The warning says the serious security vulnerability could allow "unauthorized software to be loaded on to the system."

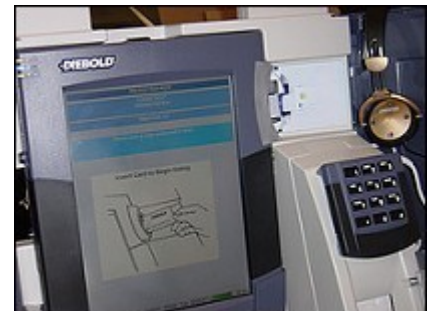
Public details about the warning are still sketchy as those in the know have acknowledged that the problem is so serious, they are hoping to keep the info under wraps until mitigation steps can be taken to safeguard systems.

The BRAD BLOG has been told on the record, however, by one person involved in the matter, that the vulnerability is a "**major national security risk.**"

We've been speaking to many sources today, and we've been able to get several first hand comments on the problem from top officials and analysts directly involved in both state and federal certification of the Diebold systems, as well as from those involved in the initial discovery of the problem.

What is clear is that *Morning Call's* reporting that it was Diebold who found the "glitch" are flat wrong. The discovery of the "glitch" (which is anything but) emanated from the examination of Diebold AccuVote TSx (touch-screen) machines recently in Emery County, UT.

A source has told The BRAD BLOG that Diebold was "cornered" into admitting to the problem, a far cry from them having "found" it, as the *Morning Call* characterized it.



What is also clear is that neither Diebold themselves, nor federal officials at the Elections Assistance Commission (EAC) have been notifying states about the serious problem which apparently affects *all* Diebold AccuVote touch-screen systems, including both their newer TSx models, and the older TS and TS6 models.

The Diebold TSx models, with the security vulnerability still intact, were apparently used in the primary election last Tuesday in Ohio.

A document at Diebold's website describes² the TSx models as featuring "Industry Leading Security."

In Utah's Emery County, state officials are attempting to force Bruce Funk, the 23-year elected County Clerk out of his job in the wake of his having allowed a security evaluation of the county's new Diebold touch-screen systems by both computer security firm Security Innovation³ and Finnish computer security expert Harri Hursti. According to several sources, that analysis revealed many new vulnerabilities and problems in the Diebold touch-screen systems, including the one that seems to be at

¹ <http://www.mcall.com/news/local/leighton/all-1schuykillmay04,0,7235865.story?coll=all-newslocalleighton-hed>

² <http://www.diebold.com/dieboldes/pdf/industrysecurity.pdf>

³ <http://securityinnovation.com/>

the heart of the problem now being warned about by Pennsylvania officials.

Funk -- who has since been "vilified," as one source told us, by both Diebold and Utah state officials as high as the Lt. Governor -- was forced to implement the new Diebold touch-screen systems for the first time this year against his own objections. His prudent subsequent security evaluation of the systems was arranged by electronic voting watchdog organization, BlackBoxVoting.org. (*We recently interviewed Funk on the radio concerning that evaluation, and his subsequent removal from office in its wake.*⁴)

Here's some of what we've so far been able to learn from a number of officials, both on the record and off, in Pennsylvania, elsewhere around the country and at the federal level, as well as those involved in the initial Emery County discoveries...

The BRAD BLOG has confirmed with a top official in Pennsylvania, close to those responsible for giving state certification of voting systems in the Keystone state, that the problem comes from a "feature" that is purposely built into all Diebold touch-screen systems.

"As far as I know, it's present on all TS and TSx machines," he told us. "It relates to potential misuse of the procedure by which Diebold does field updates to the machines. It's not a bug -- it's a deliberate but unwise 'feature'. Every jurisdiction that uses the machines should be notified. Now that the story is out, I suspect they will be. The fix can be applied at any time prior to the next election, however, so there is no particular rush except in states like Pennsylvania, which has a primary in less than two weeks. The fix is administrative and requires no new or modified software."

Bev Harris, of BlackBoxVoting.org (BBV), who described the situation as "horrifying" said in a comment posted on BRAD BLOG earlier today that, "The problem is very serious and because primary elections are being held, releasing even a small part of what makes this security hole so dangerous presents an immediate threat to U.S. elections."

She told us in a phone conversation this afternoon that BBV will be publicly publishing summaries of the full reports both from Security Innovation and Hursti on Emery County "in redacted format" soon.

"Because the vulnerability is so serious," she wrote, "and until ALL states have been able to implement the FULL recovery path, we can release a redacted version only, but will send an unredacted version to the states," she wrote in another comment earlier today.

She explained when we discussed the matter that even that "FULL recovery path" may not be possible due to the severity of the problem which she describes as "a major national security issue."

Harris wrote about a discussion last night with Dr. Michael Shamos who is responsible for testing voting systems in Pennsylvania concerning the full breadth of the security issue and the necessary means for mitigating it.

"When Dr. Shamos called me and described the mitigations being used in Pennsylvania, I have to say that they did not appear to be the full mitigation needed according to the videotaped examination we have by Security Innovation and Hursti," Harris wrote.

But whether other states and counties who use Diebold's TS and TSx machines *will* be properly notified by official federal authorities, or even Diebold themselves, is another question. Apparently the state of California has known about the problem for some time, as well as Diebold obviously, but the matter in PA seems only to have come to public attention when state officials were questioned by

⁴ Listen to that interview here: <http://www.bradblog.com/archives/00002670.htm>

Election Integrity Activists in a public meeting.

A member of the team involved in evaluating the Diebold systems recently in California on behalf of Sec. of State Bruce McPherson has told us that they've known about the problem for some time and confirmed the seriousness of the issue:

"Yes, California has definitely been aware of the issue for several weeks and will address it before the June 6 primary," the computer scientist in California explained. "Other Diebold TS and TSx jurisdictions are equally affected, and in my opinion must take ameliorating action."

Earlier this year, when McPherson was considering whether or not to re-certify Diebold in California after the Diebold optical-scan systems were revealed, in no uncertain terms, to be hackable in a Leon County, Florida mock-election test, he commissioned an independent analysis⁵ of the flaws in the Diebold memory cards which allowed for the hack to be carried out without a trace being left behind.

That report confirmed the Leon County hack, and found 16 other bugs described as "a more dangerous family of vulnerabilities" which "go well beyond" what was discovered in Leon County. Remarkably, after the report was issued, McPherson certified Diebold's systems in the state despite those dire warnings from his own security team.

Harris, however, confirms to us that the problems now being discussed in PA are an "entirely different class of problems" than were even revealed by the California report.

The Washington state Sec. of State's voting systems director, Paul Miller, has told us that when he asked a Diebold representative about the problem yesterday, the rep told him that he had no knowledge of the issue and promised to get back to him if he was able to find out anything.

When we inquired with Jeannie Layson, a spokesperson for the Elections Assistance Commission (EAC) as to whether the EAC would be notifying states about the vulnerability, she told us that their commission had nothing to do with system certification.

We reminded her that this was not an issue about certification, but rather of product security and vulnerability which needed to be passed on to every state that uses Diebold TS and TSx systems. The EAC's role in serving as a central clearinghouse for notifying states about such issues was defined by the Help America Vote Act (HAVA) which created the commission in the first place. As well, a recent 107-page report⁶ issued by the Government Accountability Office (GAO) on the problems and vulnerabilities of electronic voting (which went virtually unreported by the mainstream corporate media) discussed the EAC's role in this matter as well.

Layson told us that she would discuss the matter with the EAC's Voting System Secretariat, Brian Hancock. We look forward to action by the EAC.

John Gideon of VotersUnite.org and VoteTrustUSA.org contributed to this story

----- END -----

Reprinted by Kathy Dopp for Summit County Clerk Campaign -- KathyDopp.com

In November, I will ask voters to register their votes with a parallel citizen vote count and, if elected, I will implement independent vote count audits of voter verifiable paper ballots & detailed election data monitoring to publicly detect and correct any vote fraud or errors. See ElectionArchive.org and UtahCountVotes.org

⁵ http://www.votetrustusa.org/pdfs/California_Folder/DieboldReport.pdf

⁶ http://www.bradblog.com/Docs/GAORreport_ElectionSecurity_102105.pdf