
The Truth About Diebold

(March 30, 2006) - Contributed by Susan Pynchon, Florida Fair Elections Coalition

What A Recent Report of California Computer Scientists Tells Us About The Vulnerability of Diebold's Voting Machines
Last December, California Secretary of State Bruce McPherson asked an advisory board of computer scientists to conduct a security review of the memory card components for both Diebold's AccuVote-OS (optical scan) and AccuVote-TSx (touchscreen with voter verified paper audit printer) voting systems. The report, "Security Analysis of the Diebold AccuBasic Interpreter", which was released by the California's Voting System Technical Assessment and Advisory Board (VSTTAB) in February, confirmed numerous security vulnerabilities in Diebold's electronic voting systems. Any legislator or elections official who recommends the purchase of the Diebold TSx without reading the entire California report should be considered grossly negligent. It's hard to imagine that anyone who read this report would even consider buying anything other than optical scan voting machines. The report warns, "successful attacks can only be detected by examining the paper ballots. There would be no way to know that any of these attacks occurred; the canvass procedure would not detect any anomalies, and would just produce incorrect results. The only way to detect and correct the problem would be by recount of the original paper ballots."

The original goal of the VSTTAB scientists was to verify the results of an earlier test of voting system security that was performed in Leon County, Florida. The Leon County test, conducted by Finnish computer programmer Harri Hursti, definitively proved that election results can be altered on a Diebold voting system, without detection, by using a single memory card. The computer scientists, who conducted only a limited review of the Diebold source code, not only confirmed the validity of the "Hursti Hack" - they also discovered 16 other serious security "bugs"; each of which could be exploited to alter election results without detection.

And the report cautions that "these are just the bugs we were able to find; there are quite possibly others we did not notice". Elsewhere in the report they reiterate, "There may, of course, be additional bugs, or [different] kinds of bugs, that we did not find." The report also confirms that the Diebold TSx (touch-screen) has many of the same vulnerabilities as the optical scan system that was tested in Leon County.

The scientists wrote, "Clearly there are serious security flaws in the current state of the AV-OS [optical scan] and AV-TSx [touch-screen] software." The scientists state that the security vulnerability exploited by Harri Hursti cannot be cured by rewriting the source code. They do note that the 16 additional bugs that were uncovered, while serious and able to change election results without detection, are "easily fixable" through a code re-write, but they go on to say that the real problem lies with the Accubasic language and the "interpreted code" used by the Diebold system. The report notes: "Interpreted code in general is prohibited by the 2002 Federal Election Commission Voting System Standards and its successor standard, the Election Assistance Commission's Voluntary Voting System Guidelines due to take effect in two years. In order for the Diebold software architecture to be in compliance, it would appear that the AccuBasic language and interpreter have to be removed, or the standard will have to be changed." Since there are valid security reasons why interpreted code is not allowed under the current standards, the only legitimate action would appear to be to the removal of the AccuBasic language and interpreter. This would essentially involve redesigning the entire Diebold system.

According to the report, "Once the attacker can replace the running code of the machine, the attacker has full control over all operations of the machine. Some of the consequences of this kind of compromise could include: "The attack could manipulate the electronic tallies in any way desired. These manipulations could be performed at any point during the day. They could be performed selectively, based on knowledge about running tallies during the day. For instance, the attack code could wait until the end of the day, look at the electronic tallies accumulated so far, and choose to modify them only if they are not consistent with the attacker's wishes."

"The attack could print fraudulent zero reports and summary reports to prevent detection."

"The attack could modify the contents of the memory card in any way, including with the electronic vote counts and electronic ballot images stored on the card."

"The attack could erase all traces of the attack to prevent anyone from detecting the attack after the fact. For instance, once the attack code has gained control, it could overwrite the malicious AccuBasic object code (.abo file) stored on the memory card with legitimate AccuBasic object code, so that no amount of subsequent forensic investigation will uncover any evidence of the compromise."

"It is even conceivable that there is a way to exploit these vulnerabilities so that changes could persist from one election to another. For instance, if the firmware or software resident on the machine can be modified or updated by running code, then the attack might be able to modify the firmware or software in a permanent way, affecting future elections as well as the current election. In other words, these vulnerabilities mean that a procedural lapse in one election

could potentially affect the integrity of the subsequent election.” In addition the report notes: “It is conceivable that the attack might be able to propagate from machine to machine, like a computer virus. For instance, if an infected memory card is inserted into an infected voting machine, then the compromised voting machine could replace the AccuBasic object code on that memory card with a malicious AccuBasic script. At that point, the memory card has been infected, and if it is ever inserted into a second uninfected machine, the second machine will become infected as soon as it runs the AccuBasic script.”

“On the AV-TSx, the attack could print fraudulent VVPAT records. Since VVPAT records are considered the authoritative record during a recount [under California law], this might enable election fraud even if the VVPAT records are manually recounted.”

“In addition, most of the bugs we found could be used to crash the machine. This might disenfranchise voters or cause long lines. The bugs could be used to selectively trigger a crash only in some machines, in some geographic areas, or based on certain conditions, such as which candidate received more votes. For instance, it would be possible to write a malicious AccuBasic script so that, when the operator prints a summary report at the end of the day, the script examines the vote counters and either crashes or continues operating normally according to which candidate is in the lead.” And this just scratches the surface of what the report reveals. It is imperative that all election officials and all potential purchasers of voting systems read this report in its entirety. There are many more important points that must be understood, including the weaknesses in the Diebold system involving inadequate or nonexistent encryption codes that allow easy access to the entire system including the GEMS central tabulator.”

The tests done by the California scientists prompted Florida’s Division of Elections to issue a Technical Advisory intended to address the security vulnerabilities that were found. However, the Florida advisory is completely inadequate in that it only mandates the short-term mitigation strategies recommended by the VSTAAB report for local elections, while ignoring the recommendations for removing the AccuBasic language and interpreter before using the machines in any statewide election. To quote directly from the VSTAAB report, “While these strategies do not completely eliminate all risk, we expect they would be capable of reducing the risk to a level that is manageable for local elections in the short term. In the longer term, or for statewide elections, the risks of not fixing the vulnerabilities in the AccuBasic interpreter become more pronounced. Larger elections, such as a statewide election, provide a greater incentive to hack the election and heighten the stakes. Also, the longer these vulnerabilities are left unfixed, the more opportunity it gives potential attackers to learn how to exploit these vulnerabilities. For statewide elections, or looking farther into the future, it would be far preferable to fix the vulnerabilities discussed in this report.”

However, there is one noteworthy statement in the Florida report that says the security vulnerabilities discovered and the recommendations made in the VSTAAB report are applicable not only to Diebold, but apply “to all voting systems deployed in Florida.” That would include ES&S and Sequoia!

The most important point made in the entire VSTAAB report, in the scientists’ own words: “It is important to note that even in the worst case, the paper ballots cast using an AV-OS [optical scan system] remain trustworthy; in no case can any of these vulnerabilities be used to tamper with the paper ballots themselves.”

If you are about to purchase a voting system for your county or your state, please take this VSTAAB report to heart. The security vulnerabilities revealed by the California scientists mean that paper ballots (not VVPAT) are the only sure way to provide fair, verifiable, accurate, secure and auditable elections. Once you select an optical-scan, paper-ballot system for your jurisdiction, the next step, of course, is to guard those paper ballots like the gold in Fort Knox and require audits of a percentage of those ballots after every election. With verifiable, auditable voting systems and a secure chain-of-custody of paper ballots, the confidence of U.S. citizens in the integrity of our elections will finally be restored.