ONLINE JOURNAL™

www.onlinejournal.com

Black Box Voting

Optical scan machines hacked in Florida

By the BlackBoxVoting.org Team

June 3, 2005—Tallahassee, FL: "Are we having fun yet?"

This is the message that appeared in the window of a county optical scan machine, startling Leon County Information Systems Officer Thomas James. Visibly shaken, he immediately turned the machine off.

Diebold's opti-scan (paper ballot) voting system uses a curious memory card design, offering penetration by a lone programmer such that standard canvassing procedures cannot detect election manipulation.

The Diebold optical scan system was used in about 800 jurisdictions in 2004. Among them were several hotbeds of controversy: Volusia County (FL); King County (WA); and the New Hampshire primary election, where machine results differed markedly from hand-counted localities.

New Regs: Counting Paper Ballots Forbidden

Most states prohibit elections officials from checking on optical scan tallies by examining the paper ballots. In Washington, Secretary of State Sam Reed declared such spontaneous checkups to be "unauthorized recounts" and prohibited them altogether. New Florida regulations will forbid counting paper ballots, even in recounts, except in highly unusual circumstances. Without paper ballot hand-counts, the hacks demonstrated below show that optical-scan elections can be destroyed in seconds.

A Little Man Living in Every Ballot Box

The Diebold optical scan system uses a dangerous programming methodology, with an executable program living inside the electronic ballot box. This method is the equivalent of having a little man living in the ballot box, holding an eraser and a pencil. With an executable program in the memory card, no Diebold opti-scan ballot box can be considered "empty" at the start of the election.

The Black Box Voting team proved that the Diebold optical scan program, housed on a chip inside the voting machine, places a call to a program living in the removable memory card during the election. The demonstration also showed that the executable program on the memory card (ballot box) can easily be changed, and that checks and balances, required by FEC standards to catch unauthorized changes, were not implemented by Diebold—yet the system was certified anyway.

The Diebold system in Leon County, Florida, succumbed to multiple attacks.

Ion Sancho: Truth and Excellence in Elections

Leon County Elections Supervisor Ion Sancho and Information Systems Officer Thomas James had already implemented security procedures in Leon County far exceeding the norm in elections management. This testing, done by a team of researchers including Black Box Voting, independent filmmakers, security expert Dr. Herbert Thompson, and special consultant Harri Hursti, was authorized by Mr. Sancho, in an unusual act of openness and courage, to identify any remaining holes in Leon County's election security.

The results of the memory card hack demonstration will assist elections supervisors throughout the U.S., by emphasizing the critical importance of accounting for each and every memory card and protecting access.

Findings:

Computer expert Harri Hursti gained control over Leon County memory cards, which handle the vote-reporting from the precincts. Dr. Herbert Thompson, a security expert, took control of the Leon County central tabulator by implanting a trojan horse-like script.

Two programmers can become a lone programmer, says Hursti, who has figured out a way to control the entire central tabulator by way of a single memory card swap, and also how to make tampered polling place tapes match tampered central tabulator results. This more complex approach is untested, but based on testing performed May 26, Hursti says he has absolutely no reason to believe it wouldn't work.

Three memory card tests demonstrated successful manipulation of election results, and showed that 1990 and 2002 FEC-required safeguards are being violated in the Diebold version 1.94 opti-scan system.

Three Memory Card Hacks

1. An altered memory card (electronic ballot box) was substituted for a real one. The optical scan machine performed seamlessly, issuing a report that looked like the real thing. No checksum captured the change in the executable program Diebold designed into the memory card.

2. A second altered memory card was demonstrated, using a program that was shorter than the original. It still worked, showing that there is also no check for the number of bytes in the program.

3. A third altered memory card was demonstrated with the votes themselves changed, showing that the data block (votes) can be altered without triggering any error message.

How to "Roll Over the Odometer" in Diebold Optical Scan Machines

Integer overflow checks do not seem to exist in this system, making it possible to stuff the ballot box without triggering any error message. This would be like pre-loading minus 100 votes for Tom and plus 100 votes for Rick (-100+100=ZERO)—changing the candidate totals without changing the overall number of votes.

A more precise comparison would be this: The odometer on a car rolls over to zero after 999,999. In the Diebold system tested, the rollover to zero happens at 65,536 votes. By pre-loading 65,511 votes for a candidate, after 25 real votes appear (65,511 plus 25 = 65,536) the report "rolls over" so that the candidate's total is ZERO.

This manipulation can be balanced out by preloading votes for candidate "A" at 65,511 and candidate "B" at 25 votes—producing an articifial 50-vote spread between the candidates, which will not be obvious after the first 25 votes for candidate "A" roll over to zero. The "negative 25" votes from the odometer rollover counterbalance the "plus 25" votes for the other candidates, making the total number of votes cast at the end of the day exactly equal to the number of voters.

While testing the hack on the Leon County optical scan machine, Hursti was stunned to find that pre-stuffing the ballot box to "roll over the odometer" produced no error message whatsoever.*

*We did not have the opportunity to scan ballots after stuffing the ballot box. Therefore, the rollover to zero was not tested in Leon County. This integer overflow capability is discernable in the program itself. We did have the opportunity to test a pre-stuffed ballot box, which showed that pre-loaded ballot boxes do not trigger any error message.

Simple Tweaks to Pass L&A Test and Survive Zero Tape

Though the additional tweaks were not demonstrated at the Leon County elections office, Hursti believes that the integer overflow hack can be covered up on the "zero tape" produced at the beginning of the election. The programming to cover up manipulations during the "logic & accuracy test" is even simpler, since the program allows you to specify which reports (and, if you like, date and time of day) the manipulation will affect.

The testing demonstrated, using the actual voting system used in a real elections office, that Diebold programmers developed a system that sacrifices security in favor of dangerously flexible programming, violating FEC standards and calling the actions of ITA testing labs and certifiers into question.

In the case of Leon County, inside access was used to achieve the hacks, but there are numerous ways to introduce the hacks without inside access. Outside access methods will be described in the technical report to be released in mid-June.

Security Concerns

Putting an executable program into removable memory card "ballot boxes"—and then programming the opti-scan chip to call and invoke whatever program is in the live ballot box during the middle of an election—is a mind-boggling design from a security standpoint. Combining this idiotic design with a program that doesn't even check to see whether someone has tampered with it constitutes negligence and should result in a product recall.

Counties that purchased the Diebold 1.94 optical scan machines should not pay for any upgraded program; instead, Diebold should be required to recall the faulty program and correct the problem at its own expense.

None of the attacks left any telltale marks, rendering all audits and logs useless, except for hand-counting all the paper ballots.

Is it Real? Or Is it Memorex?

For example, Election Supervisor Ion Sancho was unable to tell, at first, whether the poll tape printed with manipulated results was the real thing. Only the message at the end of the tape, which read "*Is this real? Or is it Memorex?*" identified the tape as a tampered version of results.

In another test, Congresswoman Corrine Brown (FL-Dem) was shocked to see the impact of a trojan implanted by Dr. Herbert Thompson. She asked if the program could be manipulated in such a way as to flip every fifth vote.

"No problem," Dr. Thompson replied.

"It IS a problem. It's a PROBLEM!" exclaimed Brown, whose district includes the troubled Volusia County, along with Duval County—both currently using the Diebold opti-scan system.

This system is also used in Congressman John Conyers' home district, in contentious King County, Washington, and in Lucas County, Ohio (where six election officials resigned or were suspended after many irregularities were found.)

Diebold optical scans were used in San Diego for its ill-fated mayoral election in Nov. 2004.

Optical scan systems have paper ballots, but election officials are crippled in their ability to hand count these ballots due to restrictive state regulations and budget limitations.

The canvassing (audit) procedure used to certify results from optical scan systems involves comparing the "poll tapes" (cash register-like results receipts) with the printout from the central tabulator. These tests demonstrate that both results can be manipulated easily and quickly.

Minimum Requirements to Perform This Hack:

1. A single specimen memory card from any county using the Diebold 1.94 optical scan series. (These cards were seen scattered on tables in King County, piled in baskets accessible to the public in Georgia, and jumbled on desktops in Volusia county.)

2. A copy of the compiler for the AccuBasic program. (These compilers have been fairly widely distributed by Diebold and its predecessor company, and there are workarounds if no compiler is available.)

3. Modest working language of any one of the higher level computer languages (Pascal, C, Cobol, Basic, Fortran . . .) along with introductory-level knowledge of assembler or machine language. (Machine language knowledge needed is less than an advanced refrigerator or TV repairmen needs. The optical scan system is much simpler than modern appliances).

The existence of the executable program in the memory card was discernable from a review of the Diebold memos. The test hacks took just a few hours for Black Box Voting consultants to develop.

Nearly 800 jurisdictions conducted a presidential election on this system. This system is so profoundly hackable that an advanced-level TV repairman can manipulate votes on it.

Black Box Voting asked Dr. Thompson and Hursti to examine the central tabulator and the optical scan system after becoming concerned that not enough attention had been paid to optical scans, tabulators and remote access.

Thompson and Hursti each found the vulnerabilities for their respective hacks in less than 24 hours.

"Open for Business"

When it comes to this optical-scan system, as Hursti says, "It's not that they left the door open. *There is no door.* This system is 'open for business.'"

The question now is: How brisk has business been? Based on this new evidence, it is time to sequester and examine the memory cards used with Diebold optical scans in Nov. 2004.

The popularity of tamper-friendly machines that are "open for business" in heavily Democratic areas may explain the lethargy with which Democratic leaders have been approaching voting machine security concerns.

The enthusiasm with which Republicans have endorsed machines with no paper ballots at all indicates that neither party really wants to have intact auditing of elections.

The ease with which a system—which clearly violates dozens of FEC standards going back to 1990—was certified calls into question the honesty, competence, and personal financial transactions of both testing labs and NASED certifiers.

Revamp and update Hand-Counted Paper Ballot Technology?

Perhaps it is time to revisit the idea of hand-counted paper ballots, printed by machines for legibility, with *color-coded* choices for quick, easy, accurate sorting and counting. We should also take another look at bringing *counting teams* in when the polls close, to relieve tired poll workers.