

Diebold Voting Machine Fails New Security Test

Optical Scan (paper ballot) voting system succumbs to manipulation

New voting systems may have additional vulnerabilities



This message, which appeared on the screen of a Diebold optical scan voting machine in Leon County, Florida, startled Information Systems Manager Thomas James. He quickly turned the machine off.

“Don’t worry,” said Harri Hursti, a Finnish computer security expert brought to the U.S. by the Renton, Washington-based election watchdog **Black Box Voting**. Hursti explained, “it’s my program.”

“Poll tapes” – reports run by the voting machine at the precinct – were falsified in **Black Box Voting** tests.

```
TIME: 14:33:13 05/16/05
*****
** PRECINCT: 1 **
*****
BALLOTS CAST 222
*****
President
RACE # 10
*****
Ryan 123
Noelle 98
*****
Vice-President
RACE # 20
*****
Emily 109
Alexandra 59
Zak 33
*****
Secretary
RACE # 30
*****
Chase 125
Laura 98
*****
Treasurer
RACE # 40
*****
Claudia 64
Ashley 187
Katie 25
Brittany 27
*****
I.E. THE UNDERSIGNED,
DO HEREBY CERTIFY THE
ELECTION WAS CONDUCTED
IN ACCORDANCE WITH THE
LAWS OF THE STATE.
*****
SIGNATURES
*****
```

```
*****
ELECTION RESULTS REPORT
*****
1149 Upper School
Student Council
DATE: 04/13/05 TYPE: G
POLL CTR# 10880
*****
TIME 14:33:13 05/16/05
*****
** PRECINCT: 1 **
*****
BALLOTS CAST 222
*****
President
RACE # 10
*****
Ryan 138
Noelle 87
*****
Vice-President
RACE # 20
*****
Emily 109
Alexandra 58
Zak 33
*****
Secretary
RACE # 30
*****
Chase 111
Laura 111
*****
Treasurer
RACE # 40
*****
Claudia 200
Ashley 6
Katie 5
Brittany 11
*****
I.E. THE UNDERSIGNED,
DO HEREBY CERTIFY THE
ELECTION WAS CONDUCTED,
BUT WAS IT REAL,
OR WAS IT MEMOREY?
*****
DONT SIGN HERE
*****
```

These tapes, instead of the ballots, are used to verify results in most elections (except in rare hand recounts.)

Well, maybe that’s not so reassuring. James knew Hursti planned to attack the Diebold voting system, and was prepared for it. Hursti had been given permission by Leon County Elections Supervisor Ion Sancho to do a security evaluation. What James wasn’t prepared for was the prompt acquiescence of the voting machines to multiple attacks.

Hursti showed how, using a one-man attack, requiring just a few hundred dollars and a method requiring only modest technical abilities, he was able to gain control over voting machines – including the “poll tapes” (printouts of results from the precinct-based voting machines) and LCD screen messages. Hursti also discovered exploits to control the functions of the Yes-No buttons and to stuff the electronic ballot box, loading the machine with a manipulation to produce minus votes for one candidate and a matching number of +votes for the other, such that the overall number of votes stays the same while altering the results.

Hursti’s attacks can be implemented on one machine at a time, groups of machines, or all the machines, depending on the delivery method chosen by the attacker. Hursti used an insider’s approach, but has also identified remote attacks likely to succeed, with or without use of the Internet.

Hursti used a Diebold program called “AccuBasic” to tamper with the reports. According the technical report produced by Hursti and Black Box Voting:

“There are clear indications that more functionality is planned to be driven by AccuBasic in future releases. Thus, the role of AccuBasic appears to be increasing, not diminishing.”

Even if elections officials move to a newer version, the architecture of the system is unlikely to have changed, as it will require a major overhaul to correct the problem. Diebold touch-screens have additional vulnerabilities. Some of Hursti’s exploits were hidden so well that only a full hand recount would catch them, and then only if the chain of custody of the paper ballots themselves was intact.

The report, available for download (<http://www.blackboxvoting.org/BBVreport.pdf>) recommends that “**further evaluation** should be performed on the 1.96.x and 2.0.x versions of the Diebold optical scan system to determine whether they do or do not have the same fundamentally insecure architecture.” The report also recommends **examining the memory cards used in the Nov. 2004 election**, and obtaining a **forensic examination of the memory cards in Volusia County**, Florida, and elsewhere, where significant anomalies related to memory cards appeared in federal elections.

end