The New York Times
nytimes.com

January 31, 2004

MAKING VOTES COUNT

How to Hack an Election

Concerned citizens have been warning that new electronic voting technology being rolled out nationwide can be used to steal elections. Now there is proof. When the State of Maryland hired a computer security firm to test its new machines, these paid hackers had little trouble casting multiple votes and taking over the machines' vote-recording mechanisms. The Maryland study shows convincingly that more security is needed for electronic voting, starting with voter-verified paper trails.

When Maryland decided to buy 16,000 AccuVote-TS voting machines, there was considerable opposition. Critics charged that the new touch-screen machines, which do not create a paper record of votes cast, were vulnerable to vote theft. The state commissioned a staged attack on the machines, in which computer-security experts would try to foil the safeguards and interfere with an election.

They were disturbingly successful. It was an "easy matter," they reported, to reprogram the access cards used by voters and vote multiple times. They were able to attach a keyboard to a voting terminal and change its vote count. And by exploiting a software flaw and using a modem, they were able to change votes from a remote location.

Critics of new voting technology are often accused of being alarmist, but this state-sponsored study contains vulnerabilities that seem almost too bad to be true. Maryland's 16,000 machines all have identical locks on two sensitive mechanisms, which can be opened by any one of 32,000 keys. The security team had no trouble making duplicates of the keys at local hardware stores, although that proved unnecessary since one team member picked the lock in "approximately 10 seconds."

Diebold, the machines' manufacturer, rushed to issue a self-congratulatory press release with the headline "Maryland Security Study Validates Diebold Election Systems Equipment for March Primary." The study's authors were shocked to see their findings spun so positively. Their report said that if flaws they identified were fixed, the machines could be used in Maryland's March 2 primary. But in the long run, they said, an extensive overhaul of the machines and at least a limited paper trail are necessary.

The Maryland study confirms concerns about electronic voting that are rapidly accumulating from actual elections. In Boone County, Ind., last fall, in a particularly colorful example of unreliability, an electronic system initially recorded more than 144,000 votes in an election with fewer than 19,000

registered voters, County Clerk Lisa Garofolo said. Given the growing body of evidence, it is clear that electronic voting machines cannot be trusted until more safeguards are in place.