Paper Trail Manipulation I
Michael I. Shamos
Oct. 5, 2005

Taxonomy: wholesale, paper-trail subversion
Applicability: cut–sheet paper trails that print non-human-readable indicia

Method:
To prevent ballot-box stuffing with forged ballots, most "voter-verified" paper-trail systems print one-or two-dimensional barcodes or cryptographic indicia, on the verified ballot. The indicium is usually a computed function of the content of the ballot, e.g. a hash. The indicium may also contain a pointer to the electronic record that is supposed to correspond to that specific ballot. In the event of a recount, legitimate ballots will possess the correct indicia, while a forged ballot will not.

Assume that the code in the voting machine has been subverted as follows: the system always produces accurate voter-verified ballots, but when a voter votes for candidate A, then with probability p the barcode or indicium is printed incorrectly and no electronic record is made of the ballot. The voter believes the ballot is correct, and therefore indicates that the vote should be recorded. The ballot is automatically dropped into the ballot box. After the voter leaves the machine, a new ballot is printed with a vote for candidate B with a correct indicium and an electronic record of this ballot is made. The second ballot is also deposited automatically in the ballot box. This effectively switches a vote from A to B.

When the polls are closed, the software removes all trace of the manipulating code so an inspection of the software after the election will not reveal anything amiss.

The method will not be successful with continuous-roll paper trails. Because of the physical integrity of the paper roll, there will be no rational explanation how ballots with incorrect indicia became interspersed.

Resource requirements: The perpetrator must be intimately familiar with the voting machine code and be in a position to substitute what amounts to a Trojan horse for the legitimate software.

Potential gain:

Massive, depending on the extent to which the manipulation is deployed. Care is required in selecting which races to manipulate, and by how much (i.e., the choice of A, B and p). If the swing is too lop-sided, great suspicion will be raised, but it is not clear what can be done about it.

Likelihood of detection:

If there is no recount, the manipulation will not be detected. If the ballot box is opened and the ballots are counted, a discrepancy will be observed between the number of voters who voted and the number of ballots in the box. Unless the ballots are individually examined, it will not be possible to distinguish the extras from ordinary spoiled ballots.

If a recount is performed, invalid ballots will be present. The number of valid ballots, however, will match the number of voters and the electronic count will match the valid ballots exactly. It is possible that the correct conclusion will be drawn that software tampering has occurred, but since the software has erased any trace of the intrusion, it will not be possible to prove. With the electronic count and the physical count being equal, the intrusion will have succeeded.

Countermeasures:
Preventative measures:

Careful code evaluation at qualification testing and chain of custody of executables that actually get installed in voting machines. Wholesale fraud can occur at the vendor, the distribution point or the county warehouse. Successful manipulation of individual machines after delivery to the precinct is difficult because of physical interlocks and results in retail fraud even if it occurs.

Detection measures:

The printing of the second ballot when the first has been invalidated can be detected aurally.

Parallel testing will also reveal this exploit.

Retrospective:

So-called "voter-verified" paper trails are not actually voter-verified. The paper record should not contain any information that cannot be read or understood by the voter yet can be used to invalidate the ballot when a recount is performed.