Paper Trail Manipulation II

Michael I. Shamos
Oct. 5, 2005

Taxonomy: wholesale, paper-trail subversion
Applicability: all paper trails that the voter cannot touch, whether cut-sheet or continuous roll

Method:

Under HAVA, a voter must have the opportunity to spoil a ballot and vote again. With paper trails, this is implemented by having the system void the paper ballot if the voter does not agree with its contents.

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 ballot is voided by the machine even though the voter indicates assent, and no electronic record is made. After the voter leaves the machine, a new and non-voided ballot is printed with a vote for candidate B and an electronic record of this ballot is properly 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.

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:

This manipulation will not be detected other than through parallel testing. The voided ballots will appear simply as normal spoiled ballots. The electronic count will match the physical count and nothing will appear extraordinary.

The method will not work with cut-sheet systems in which the voter physically deposits the ballot in a box herself. In such systems the machine has no opportunity to void the original ballot or print another.

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.

Paper trail systems must be designed physically (not just in software) to prevent this exploit, that is, in such a way that a voter's ballot cannot be marked void without the voter knowing about it

Detection measures:

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

Parallel testing will also reveal this exploit.

Retrospective:

So-called "voter-verified" paper trails are not actually voter-verified unless the voter is able to satisfy herself that the ballot she verifies is not later manipulated or replaced.