

EXAMPLE ATTACK DOCUMENTATION

Optical Scan Configuration File

Douglas W. Jones

Sept 15, 2005

Taxonomy: Administrative, wholesale

Applicability: All voting systems

Method:

Typical mark-sense ballot scanners have a single mark sensing mechanism positioned over each column of the ballot, plus a sensor that scans down a column of index marks to sense what row of the ballot is passing under the scanning head. Thus, the scanner does not sense a vote for a particular candidate, by name, but rather, it senses a mark at the intersection of a particular row and column. The ballot text sent to the printer specifies the candidate name to be printed next to each voting target, and it specifies the positions of the voting targets. The vote tabulator does not read the text of the ballot, but rather, it must be configured, using a configuration file, so that it can relate the coordinates of marks it finds on the ballot to the names of the candidates. This mapping is sometimes a two-level mapping from ballot coordinate to candidate number, and then from number to name.

If the perpetrator can edit the ballot configuration file for a precinct, the perpetrator can do such things as making the scanner credit one candidate with votes intended for another.

Resource requirements: The perpetrator must gain access to the configuration files. These files are typically exposed in the computer system used to prepare the election, so they are available to the technicians setting up the election. Typically, these files are transferred to the mark-sense tabulator using removable media such as disks or PCMCIA cards. Anyone with access to these media could potentially attack the system.

For precinct-count mark-sense systems, attacks on one precinct could be done by someone who has access to these media before the polls open.

Potential gain:

All votes cast on the machines that have been may be corrupted. A serious thief must consider how to avoid being noticed. Adjusting the configuration files so that votes for one or more minor party candidates will be added to the total for a major party candidate is probably the safest attack. Another moderately safe attack is to exchange the totals for two candidates who are expected to attract comparable totals.

Likelihood of detection:

So long as the tinkering is done carefully, the likelihood of detection is small.

Countermeasures:**Preventative measures:**

Authentication of the configuration files can protect against outsiders attempting this attack. This does not protect against insiders with access to the configuration files prior to their being authenticated, so voting system designs that prevent access to these files should be preferred.

Secure transmission of configuration media can help. Configuration files should not be loaded into voting machines if those machines are left in insecure locations for extended periods before the polls open.

Optical scan systems that actually read the ballot instead of just looking for marks at designated locations would be possible. It is conceivable that such scanners could be designed so that there was no need for a configuration file.

Detection measures:

Report vote totals by ballot position as well as by candidate name. This would expose the contents of the configuration file in the canvass, so that anyone could compare the positions reported in the canvass with the actual positions on the ballot.

Pre-election tests can help, but only if the test is performed with the same configuration file as is used in the real election, and only if the test includes different numbers of votes for each candidate, in order to assure that the vote totals for candidates are not exchanged.

Post-election auditing can help, for example, following the California law where one percent of all precincts, selected at random,

are recounted after each election.

Recount laws that allow a hand recount of the actual ballots are an important defense. Recount laws that require use of the same tabulating equipment and the same configuration files as used in the first count serve to actively prevent detection of this category of error.

Citations:

Configuration file errors have been noticed on DRE and optical scan equipment. Franklin County Indiana had such a problem in 2004, in which straight party Democratic votes were credited to the Libertarians.

Inadequate pre-election tests that could not detect this type of tinkering are widespread. See

<http://www.cs.uiowa.edu/~jones/voting/miamitest.pdf>
(section 1, pages 1 to 3).

Retrospective:

There is no widespread understanding of the number of levels of indirection in the linkage between ballot marking location and candidate name. This comment applies equally to all electronic voting technologies from the Votomatic to the newest touch-screen voting systems.