

Appendix C

[of Stanley A. Klein, Position Paper on Voting System Threat Modeling,

September 24, 2005]

Exploitation of Compromising Electromagnetic Emanations

Taxonomy

Retail, vote buying, or voter intimidation.

Applicability

DRE voting machines. Possible use against precinct-based optical scan tabulators.

Method

Perpetrator uses compromising electromagnetic emanations from voting machines to reproduce DRE screens in a vehicle near the polling place. Bought or intimidated voters are instructed to make certain combinations of selections and changes to enable the perpetrator to identify which voter is using which machine. Perpetrator watches the machine activity and ensures that voters vote as instructed. This attack effectively returns voting activity to the conditions that existed prior to adoption in the late 1800's of the Australian Secret Ballot.

Exploitation of emanations from an optical scan tabulator would require either (a) the voter being instructed to vote in particular ways for offices/issues not of interest to the perpetrator, or (b) administrative records accessible to the perpetrator or an accomplice inside the polling place who can provide information on the sequence of voters whose ballots are being processed.

Resource Requirements

This attack requires development of software to monitor and process the compromising electromagnetic emanations. This development has economy of scope; once developed, the hardware and software can be reused in numerous elections. The cost of developing and producing the relevant equipment is likely to be in a multi-million-dollar range, but over time the relevant technology is likely to become ubiquitous.

The relevant technology may already exist and be in use within the intelligence community. The feasibility of exploiting compromising electromagnetic emanations from electronic equipment has been rumored since the 1970's. The Defense Department has long had a program called "Tempest" for minimizing compromising electromagnetic emanations from electronic equipment. Redacted Tempest documents were posted on the Internet a few years ago as a result of a FOIA request.

The technology requirements for accomplishing the attack are likely to include the following:

- High capacity software defined radio
- Digital signal processing and/or directive antenna technology (such as phased arrays) sufficient to separate individual voting machine emanations. For example, this might be done by using small differences in clock speeds or other processing hardware characteristics of the various machines.
- Digital signal processing to reconstruct the internal processing and screen displays from the voting machine emanations.

The software defined radio and high capacity digital signal processing technologies are currently available, although not necessarily at low cost and sufficiently small size to allow installation of the necessary facilities in a vehicle. These technologies at appropriate capacities, sizes, and costs are likely to become ubiquitous during the lifetime of voting machines in current service or currently being designed and purchased.

Perpetrators must also have access to a pool of subvertible voters willing to vote in return for payment or unable to complain if threatened. Employees, tenants, and those with similar dependency relationships are particularly vulnerable.

Potential Gain

One vote per subverted voter.

Likelihood of Detection

The likelihood of detection depends on the degree of dependency linking the perpetrator to the subverted voters.

Countermeasures

Preventive Measures

Apply to voting machines and polling places the Tempest technology and other measures used by the Defense Department for protecting against exploitation of compromising electromagnetic emanations.

Use only optical scan machines, and take measures to block the collection of information that could identify the sequence of voters whose ballots are being scanned.

Detection Measures

The attack can not be detected by technical or administrative means. The only possibility of discovering that it has occurred is if one of the voters reveals the existence of the vote buying or voter intimidation to authorities who are not themselves involved in the scheme.

Citations

None

Retrospective

None.