

## **Appendix B**

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

**September 24, 2005]**

### **Smartcard Port Attack**

#### **Taxonomy**

Retail if performed by a voter or polling place official in the polling place. Wholesale if performed by an insider during or subsequent to machine setup.

#### **Applicability**

DRE voting machines using smartcards for voter authorization and other functions.

#### **Method**

By creating an appropriate interface, an attack on a voting machine can be based on software resident on another device. Modern cell phones and personal digital assistant (PDA) devices contain computers suitable for such an attack. An example of this kind of attack would be to penetrate the voting machine electronically through a smartcard reader port, often used in DRE machines for voter authorization. The device interface software that would be the focus of this attack is likely exempt from inspection under the provisions of VVSG Volume 1 Section 1.6 because of status as unmodified "Commercial Off-The-Shelf" software. Plans for an electronic device that connects a computer to a smart card reader port can be downloaded from the Internet (at <http://www.electronic-lab.com/projects/misc/003/>). An attack can be pre-programmed by experts, making it necessary for the attacker only to place a device into the smart card reader and remove it. The relevant electronics can be made easy to hide in clothing and the connection to the device in the smartcard port can be made by thin cable or optical wireless, making it very difficult for polling place officials to see that the attack is taking place. The attack could be perpetrated for various malicious purposes either in the polling place or during pre-election setup.

The external computer subverts an exploitable smart card driver and gains access to the voting machine memory bus. Programs on the external computer are then run to accomplish the purposes of the attack. For the retail polling place attack, this would be to

“edit” previously cast ballots. Examples of wholesale (post-setup attack) purposes could be to maliciously modify the voting machine setups or to load self-deleting malicious software onto the machines.

## **Resource Requirements**

This attack requires development of the smartcard emulation hardware, the interface to the external computer, and the attack software resident on the external computer. 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 can probably be performed by someone with electronics expertise for an amount ranging from under \$100 to as much as \$1 Million depending on the sophistication of the interface (e.g. ease of concealment) and number of devices produced.

Also required are perpetrators to execute the attacks. For retail attack, these can probably be recruited and trained at low cost. An insider executing an attack at setup time would probably have to be bribed or otherwise induced to perform the attack.

## **Potential Gain**

For the retail attack, all the votes on each attacked machine can be modified. For the wholesale attack, all machines in a jurisdiction set up at the same facility could be loaded with malicious software.

## **Likelihood of Detection**

Depending on the sophistication of the design and the training of the perpetrators executing the attack, this attack could be extremely difficult to detect.

## **Countermeasures**

### **Preventive Measures**

1. Eliminate use of smartcards.
2. Provide means to disrupt any connection between the smartcard emulator and the external computer. (This can create an escalating “arms race” of increased sophistication in prevention and attack technology. For example, in the 1990's

European telephones contained cable cutters to prevent a similar kind of attack. Attackers countered by using thinner cables.)

3. Ensure that the voting machine operating system and the smartcard driver are not exploitable. This will require removing any "COTS Exemption" from all relevant software and conducting penetration tests of attacks through the smartcard port.

### **Detection Measures**

None, if attack has sophisticated design.

### **Citations**

Smartcard emulation attacks on telephone systems were described in an article appearing in 2600 Magazine in 1996 or 1997.

### **Retrospective**

None.