Stanley A. Klein

7 Lorre Court

Rockville, Maryland 20852

sklein@cpcug.org

301-881-4087

September 24, 2005

Position Paper on Voting System Threat Modeling

Voting is the most critical and fundamental process of a democratic society, a process from which "the consent of the governed" and thereby all governmental authority is derived. Voting systems must be required, designed, tested, operated, monitored, and certified to be reliable, accurate, secure, usable, and auditable. Systems should be so designed that errors and malfunctions are recoverable, that any malicious tampering is both detectable and recoverable, and that ordinary citizens are fully capable of understanding, observing, and knowledgeably participating in all processes and procedures necessary to ensure these attributes.

Voting systems have been clearly and repeatedly demonstrated to be seriously insecure and vulnerable to malicious tampering. We need to view the fraudulent takeover of government power by cybercriminal stealth just as seriously as we view the wrongful takeover of government power by force and violence. In a 4-year election cycle, roughly $2 Billion to $3 Billion is spent to influence the outcome of elections. If ruthless, unscrupulous interests diverted just a single digit percentage of that money to developing and executing technically sophisticated attacks on voting systems, the aggregate expenditure could exceed a quarter billion dollars. This is not just an abstract possibility -- some individuals, reporters, and researchers have alleged that attacks at various levels of sophistication have already affected results in recent Federal and state elections. Valid or not, the allegations are within the envelope of technical and operational feasibility.

Threat modeling is part of the technology developed over the past 30 years for properly protecting computer systems that includes the Defense Department “Orange Book” and the Common Criteria (International Standards Organization standard ISO-15408). NIST is a primary center of expertise in this technology. A threat model that could be used as a basis was provided in Section 5.1.2.3 of IEEE P1583 draft 5.3.2 that was provided to the TGDC. The text of that threat model is reproduced as Appendix A to these comments.

The threat model clearly states that governmental power is the asset requiring protection in voting machine security and that those attempting to compromise election integrity are likely to be highly motivated, technically expert, and well-financed. The potential pool of threat agents is

identified as including personnel of voting machine manufacturers and their suppliers, election administrators, political operatives, and polling place personnel. Based on allegations of malicious tampering in recent elections, the threat agent pool potentially attempting to influence elections by cybercriminal stealth should be expanded to include law enforcement officials, former operatives of US and foreign intelligence communities, and organized crime.

The development of attack technology has economy-of-scope. Once a few million dollars are spent developing an attack on a particular voting system, that attack technology can be reused for the lifetime of the system in every jurisdiction where that system is used.

A proper threat model should address conditions over the intended lifetime of voting equipment. The lifetime expected by current purchasers of voting systems is likely in the range of 20-30 years. Accordingly a threat model should look forward to identify attack technologies likely to exist 15 to 25 years in the future. Examples of these threat considerations include:

- Reduced cost, increased capability, and increasing ubiquity of technologies for processing and exploiting compromising electromagnetic emanations. This issue is reflected in the threat model of Appendix A at item (d)(3).
- Reduced size, reduced power consumption, and increased capability of digital electronics. This will make it much easier to conceal attack equipment on the person of a voter or insider.
- Increased capability for attacking wireless systems, including optical wireless, at greater distances and with greater sophistication.

The threat model of Appendix A could probably serve as the basis of a wide variety of individual attacks. Appendices B and C provide outlines of two attacks: an attack through the smart card port (illustrating item d(5) of Appendix A), and exploitation of compromising electromagnetic emanations (illustrating item d(3) of Appendix A). The outlines are provided in the format requested on the NIST web page.

Appendix A

Threat Summary from IEEE P1583 Draft 5.3.2 (provided to EAC/TGDC)

5.1.2.3 Threat Summary

This section lists generic threats to which a voting system may be subject. It is, of course, not possible to enumerate all threats, but this establishes a lower bound on the threats that must be defended against.

Assumptions:

a. The persons who may be attempting to compromise the election process, and thereby the voting equipment, may be well-financed.

b. Given adequate unmonitored access there are motivated people who have the training and ability to compromise the election equipment.

c. The need for anonymity (where required by cognizant authority) of voter ballot reduces or entirely removes many traditional forms of auditing commonly used for other electronic systems (such as ATMs in banks).

d. Strong physical security is required to prevent unauthorized or unmonitored access during unattended storage periods.

e. For elections, the principal asset is governmental power. That power is transferred by the results of counting voted secret ballots. Hence, integrity of the voted ballot is critical through the entire process from capturing the voter's intent, casting it into the ballot box, counting it to produce the election results, and finally retaining it to resolve disputes.

f. The persons attempting to compromise the election process could be insiders with full knowledge of the election system including, but not limited to, political operatives, vendor personnel, polling place workers, or election administrators.

Threats: The principal vulnerabilities to the voted secret ballot are (1) undetected compromise of election integrity, (2) compromise of ballot secrecy, and (3) denial of voting service. All threats to voting systems can be classified under one or more of these vulnerabilities.

a) Software Development, Testing, and Distribution phase

1) A programmer embeds a backdoor or other software in a COTS product known to be potentially used in voting systems that enables malicious code to be later inserted into the voting system.

2) A programmer embeds code into the voting system software that directly or indirectly (such as by allowing later introduction of malicious code) allows one or more of the following to be done at a later time:

   i) Recording a ballot different from the ballot displayed and entered by the voter, either consistently or with intentional pseudo-randomness.

   ii) Modification of previously recorded votes or of vote totals

   iii) Causing a machine to become inoperable for further voting

   iv) Casting ballots that did not come from legitimate, authorized voters

   v) Observing recorded votes or vote totals prior to the time authorized.

   vi) Modifying audit trails

   vii) Identifying ballots cast by specific voters, with or without collusion of the voters involved.

   viii) Causing a machine to fail completely or to incorrectly record votes either generally or according to some logic.

   ix) Disabling features required for enforcing legal requirements of the ballot style or enabling features not permitted under legal requirements of the ballot style.

   x) Calculating vote totals inconsistent with legal requirements of a ballot style.

3) A vulnerability or other non-deliberate error in the development of a COTS product potentially used in voting systems enables malicious code or erroneous data to be later inserted into the voting system.

4) A vulnerability or other non-deliberate error in the development of a voting system has an effect similar to that identified in a-2.

5) Some systems are manufactured as to be subtly different from others such that malicious modifications can be made or deployed more easily.

b) Inter-Election Maintenance phase

1) An insider (election official or voting system technician) inserts malicious code into the software having an effect similar to that identified in a-2.

2) Someone who has illegally gained access to the voting systems (who is not an insider) modifies the devices. (This could also be true at any of the other points, but is most likely to happen during the months between elections where controlled access to the systems may be lax.)

c) Election Setup phase

1) An insider inserts code into the software and/or data into the election setup that causes item (a) of a-2 to be part of the election setup or to be introduced later and allows the remaining items of a-2 to be performed later.

d) Voting phase

1) A voter is able to insert malicious code or otherwise tamper with the voting device to cause or perform any of the items listed in a-2.

2) An insider is able to insert code or otherwise tamper with, e.g., adjust, the voting device or with any stored data that causes, performs, or allows any of the items listed in a-2 whether deliberately or inadvertently.

3) An eavesdropper is able to use compromising electromagnetic emissions to identify or modify ballots cast by voters, with or without collusion of the voters involved.

4) A voter, technician, poll worker or election official may be able to activate a Trojan horse or other malicious code that has been previously installed, in order to affect or manipulate ballot contents or vote.

5) An external device may be connected to the voting system through smart card or other external interface and allow unintended actions to occur.

e) Post election phase

1) Tampering having occurred with the voting system during the election, an insider is able to remove the tampering so it will not be detected.

2) Tampering is designed as to be self-removable such that it deletes any evidence of itself following its triggering or at the end of the election.

f) Data can be selectively activated and run as alternative code at any point in the election process.

Appendix B

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.electronics-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.

Appendix C

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 subvertable 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.