CS261 Computer Security

Lecturer: David Wagner

Notes: Hong Hu

11-2-2009

Voting machine (DRE)

Voter's attacks: what the regular voters can do:

1. Goal of security:
    a. Can't vote twice by authenticating a token (smart card)
    b. Can’t remove external memory card, can’t tamper with the data on the memory card
2. Work flow:
    a. Voter comes and register with the poll worker
    b. Voter is provided with a smart card
    c. Voter insert the smart card into the voting machine
    d. Voting machine authenticates the smart card (see below), allowing the voter to vote
3. Problems:
    a. Authentication protocol of smart card

i. DRE: who are you
ii. Smart card: voter card
iii. DRE: active?
iv. Smart card: yes
v. Vote
vi. Deactivate the smart card

b. Problem: Relying on smart card for all these information, which can be easily fabricated
c. Defenses: authentication using private keys or symmetrical keys so that DRE can verify the content of smart card comes from a trusted source
d. Defense can typically be broken by physical access to the machine
    i. Tampering with the code
    ii. Gain access to all the private keys
e. Physical tampering is very powerful. Cannot rely on machines to do it. State-of-the-art safe can only handle 30 min of physical tampering by someone with tools and explosives
    i. Have to manually restrict the physical access

Massive attacks:

1. Voters attacks are more or less insignificant in big elections, large scale attacks are possible with much more dire consequences
2. Virus:

    a. DRE reads a particular file on the memory card as software update without proper authentication
    b. This allows malicious users to install arbitrary firmware on DRE through a simple memory card insertion
    c. What's worse is that compromised machine can infect all memory cards that's inserted in it, thus spreading the virus on a large scale
    d. Compromised machine can produce arbitrary election results
3. Failure of security by obscurity
    a. History of how the vulnerability is discovered in the first place
    b. Government officials and machine manufacturers refuse to fixe the problem in a prompt manner, as result of many complex factors
    c. Problem still persists at current state
4. Fundamental flaw is that the devices and memory cards more or less trust each other without proper authentication.

Another defense:

1. Print an actual piece of paper that can be recountable accompanying electronic voting. Have voters verify the paper, collect the paper
2. After election, random sample a subset of machines and manually count paper counts to obtain some statistical probability of a possible attack
3. If possible fraud happens, re-count all paper
4. Potential problems: human factor, people don't really verify the paper