Wi-Fi Usage in Voting (without inside assistance)

Jeremy Epstein

Sep 29, 2005

Taxonomy

Wholesale.

Applicability

Voting phases: Any system using Wi-Fi (typically but not exclusively DREs), whether or not the Wi-Fi is intentionally used. There is at least one model of DRE that uses Wi-Fi (the AVS WinVote); there may be others. Additionally, since many DREs are based on off-the-shelf laptop computers which have built-in Wi-Fi[1], there may be products that have Wi-Fi capabilities that are not advertised, and perhaps not even known by the DRE vendor.

Method

Many voting machines use Wi-Fi (wireless networking, typically following the IEEE 802.11b or 802.11g standards) for communication among machines in a precinct. In some cases, they are used for opening and closing the polls, while in other cases they might be used during the day.

This example assumes that the perpetrator has no ability to affect the software in the voting machine prior to election day (a "life cycle" attack), but rather is working strictly as an outsider. Many of the issues are the same as in a life cycle attack.

The initial goal of the attacker is to get access to the machine via the Wi-Fi connection, followed by any of the other typical types of attack (e.g., to modify the vote totals, modify the programming, or make the machine fail). For example, the programming could be modified to add every fourth vote for Jane Jones to the total for Sam Smith instead, while displaying the correct values on the screen.[2]

In some cases, vendors assert that the Wi-Fi capability is turned off at all times, or except during poll opening and closing. In that case, an additional attack method may require

---

[1] Nearly any laptop using the popular Pentium M chipset will have Wi-Fi.
[2] Such actions have happened by accident in voting system demonstrations. Whether they have happened in real elections is unproven, but is a matter of debate.

determining if the Wi-Fi hardware has remote "wake-up" capabilities, which allow enabling the device by sending a particular unpublished message.[3]

Resource Requirements

The perpetrator must have the ability to send Wi-Fi signals to the voting systems, which must have hardware to receive those signals. Further, the software in the voting system must have one or more vulnerabilities that allow using (or abusing) the Wi-Fi communications.

Potential Gain

- Ability to shut down as many precincts as can be visited on election day by the perpetrator and his/her co-conspirators (known as a "denial of service" attack).
- If vulnerabilities exist in the Wi-Fi capability, ability to make arbitrary modifications to the voting totals at as many precincts as can be visited on election day by the perpetrator and his/ her co-conspirators.

Likelihood of Detection

The likelihood of detection is very low, as the attacker need not be inside the polling place to launch attacks. A Pringles® potato chip can is a highly effective receiver for Wi-Fi traffic[4], allowing access from a substantial distance (e.g., a car driving within several hundred yards of the precinct). Further, it would only take a few seconds to modify the programming if the Wi-Fi implementation is vulnerable to attack, thus allowing the attacker to perform the reprogramming without even parking his/her car.

The difficulty is not access to the Wi-Fi signal, but rather the question of whether the Wi-Fi device is enabled (or can be remotely enabled) and whether the software using the Wi-Fi device has vulnerabilities. Assuming that the vulnerabilities exist, the chance of detection is very low.

Encrypting the Wi-Fi traffic (the most commonly described protection for Wi-Fi) is not a countermeasure to this type of attack.

Countermeasures

Preventative Measures

---

[3] Some network cards for wired networks have this capability. Whether Wi-Fi hardware has a similar capability is a supposition on the author's part.
[4] A report in 2001 gave the cost of building a Pringles® antenna at under $7 each, or less if built in bulk. See http://www.oreillynet.com/cs/weblog/view/wlg/448 for details.

Source code review may be able to find flaws that allow inappropriate use of Wi-Fi hardware. However, source code review is only moderately effective even when security flaws are accidental. Additionally, even the voting system vendors do not have the source code for much of their systems (e.g., the operating systems and device drivers which are a potential weak spot for Wi-Fi implementations).

Requiring hardware for voting machines that does not have any Wi-Fi features completely prevents this type of attack. As Wi-Fi is increasingly built into laptop computers (the basis for most DREs), this is increasingly infeasible.

Having all voting machines inside a Faraday cage, such as is used for processing classified information (where it is known as a SCIF). This would require that the attacker be inside the same facility, making a remote attack impossible. Equipping every precinct as a Faraday cage is impractical, and putting each voting machine inside a Faraday cage is equivalent to disabling the Wi-Fi, thus eliminating any benefit it might have.

Detection Measures

Detection is difficult if the modifications made in vote totals are relatively small, but a 5% change in vote totals could easily be made without detection.

Voting systems that provide a paper backup (e.g,. optical scan or DRE with VVPAT) can be recounted; a hand recount would detect any tampering.

If the attacker adds ballots rather than modifying those that have already been voted (or are yet to be voted), then a reconciliation of the number of votes vs. the number of voters will detect the attack.

Citations

None.

Retrospective

This is a variation on stuffing the ballot box. It does not require physical access to the voting machine, and operates by replacing ballots rather than adding new ones.