

Security Risks associated with pre-election delivery of Electronic Voting Machines

Barbara Simons

Attack names: hacking voting software and disenfranchising voters.

Applicability: security risks deriving from early delivery of voting machines.

Attack method: see below.

Resource requirements and costs: a successful hacking attack would require tamper proof tape and a device to place numbers on that tape similar to that which is used by the county. The disenfranchisement attack requires only the ability to access the machines the night before the election.

Consequences and potential gain: in a close race, the outcome of the race could be affected. If some of the techniques, eg disenfranchisement, were widely used, the impact could be more significant.

Likelihood of detection: see below.

Countermeasures: It's not clear how to avoid early delivery of voting machines, given the large number of machines that need to be delivered, combined with the need to charge the batteries prior to the election. Stronger security might reduce the risk of pre-election hacking of the software. But the disenfranchisement attack seems very hard to protect against, unless the machines are kept under lock and key until Election Day or there is an alternative method for voting. In my opinion, the obvious response to the disenfranchisement attack would be to provide adequate paper ballots to every polling station to allow the election to proceed in the absence of voting machines. A key countermeasure would be the passage of legislation that would mandate that an election be rerun in the event that tampering has been detected.

Citations and References: NA

Retrospective and Historical Notes: NA

Background.

I served as a polling station inspector in Santa Clara County, California, in the November 2004 election. My polling station was a commons room in a dorm on the Stanford campus. The set of attacks I describe range from small scale (hacking individual machines) to medium scale (disenfranchising voters in selected precincts).

Unfortunately, the general problem of delivering DREs prior to Election Day and storing them securely until Election Day is widespread.

How the machines were delivered and set up.

Santa Clara County delivered five Sequoia paperless DREs to the commons room a week before Election Day. When the woman who made the space available for the election arrived at work that morning, she was horrified to find that the machines already had been delivered. She had asked the county to deliver the machines after she had arrived at work, so that they could be placed in a secure room. Since her request had been ignored, she arranged for the machines to be moved into her office, where she kept them under lock and key until the night before the election. Obviously, the janitor had a key to her office. I don't know who else had a key. Even if her office were completely secure, she or potential co-conspirators would have had plenty of time to access the voting software. (I don't for a minute think that any of this happened. I'm simply pointing out the risks).

We poll workers met at the dorm the evening before the election. We were tasked with organizing the room for the election and with setting up the voting machines in a preliminary state so that the batteries could be fully charged. Because most polling stations do not have a large number of electric outlets, the machines are designed to be daisy chained. In other words, one machine is plugged into an electric outlet, the second is plugged into the first, the third into the second, and so on.

When initially delivered, the machines were "protected" by two levels of tamper proof tape, each piece of which had a unique number. The first level was to be removed the night before the election, when we did the initial set-up. The second level was to be removed on Election Day when we initialized the machines.

Prior to daisy chaining the voting machines, we had to remove the first level of tamper proof tape. The individual pieces of tape were stored in a plastic bag that had been provided by the county. Once the set-up work had been done, we went home. The machines were left unattended in the unlocked commons room.

We returned early the next morning to initialize the machines for Election Day. Prior to the initialization, the second level of tamper proof tape was removed and retained in a plastic bag. All of the removed tamper proof tapes were included in the material that we returned to the county election officials on election night.

Security risks of the procedures deployed by Santa Clara County.

There are multiple security risks, depending on the goal of the attacker. They require differing assumptions about the tamper proof tape and include:

1. Hacking the voting machine software without being detected. This could have been done either by someone who had access to the machines when they were in the commons room, or by someone who had access to the office where they were stored a few hours after delivery. It would be necessary to acquire identical tamper proof tape and a device to mark the tape. However, tamper proof tape is commercially available. It might even be possible for a "mole" working for the county to smuggle out some of the tape.
2. Hacking the voting machine software and risking detection. Since we poll workers had never seen the tamper proof tape and had no idea of what the numbers on the pieces of tape should be, we would not have been able to

- determine that someone had hacked the software and replaced the original tapes with different tamper proof tapes. This attack might be detected by election officials if they review the tapes that we returned. Of course if the attacker happened to acquire identical or nearly identical tape and if the attacker used the same number on the counterfeit tapes as had been on the original tapes, it's likely that even diligent election officials would not detect the fraud.
3. Targeting specific precincts in a denial of service attack. This would have been a very easy attack, since the machines were left in a publicly accessible location the night before the election. All that would be required would be for the attacker to remove the second level of tamper proof tape. Poll workers had been instructed to request new voting machines if the tamper proof tapes had been removed. Had we requested new machines, we certainly would not have had the machines up and running by the time the polls were scheduled to open. Indeed, we were barely ready by opening time, even though we had all arrived at the dorm an hour early. I don't know how many machines the county had in reserve, but if there were a widespread attack that removed the tamper proof tape from machines in many voting stations, it is highly likely that the county would have been incapable of replacing the suspect machines.

A related issue is what would happen if hacking or tampering had been detected after the election. As we saw with the butterfly ballots in Florida and in the lost votes in Carteret County, N.C., we do not have adequate legislation for dealing with situations in which election problems are detected after an election. Had tampering or hacking been detected in the presidential race, it is unlikely that the election would have been rerun. The result would have been to raise questions about the validity of reported results and to increase the cynicism of the voting population.