CS 261- 11/27 Instructor: David Wagner Scribe: Armando Solar-Lezama

Voting Systems.

Before we can analyze electronic voting systems, it is useful to look back at how elections used to be run.

Voting in the precomputing era.

Voting in the precomputing era could be divided into three different stages.

Stage 1. Show of hands vote. In the early stages of democracy, most voting was done through a show of hands. While this style of voting had the advantage of making independent validation possible---since anyone could do an independent count of hands---this style of voting introduces the possibility of coercion. This is because a corrupt agent who wishes to influence the vote can coerce people to vote his way, and can easily verify whether they actually did so. This prevents people from voting their conscience.

Stage 2. Voting through non-standardized ballot. Around the 1800s, show-of-hands voting began to give way to the secret ballot. The idea was simple; you write your choices in a piece of paper, and deposit the paper in the ballot box. This was supposed to shield people from undue coercion by making their vote secret. However, this style of voting had numerous vulnerabilities. The first problem was that the secrecy of the ballot depended on the voter actually wanting to keep his vote secret. In other words, voters could intentionally display their voting choice by voting with an especially marked ballot. Thus, a corrupt agent could coerce you to display your voting choice by forcing you to vote with a pre-marked ballot that was easy to identify, or by requiring you to sign your name on a ballot so it could be identified during the count. In fact, during this stage it was common for political parties to issue ballots that were pre-marked with the party slate and that were conspicuously colored so a party official could be sure that you deposited the ballot that was issued to you. A second vulnerability was that newspapers could influence the vote by printing “convenience” ballots containing only the names of the candidates they liked. Thus, poorly informed voters would simply use these ballots, and select among the candidates shown in the ballot, giving these candidates an edge over the other candidates.

Stage 3. Australian secret ballot. An important innovation on ballot-voting came in the mid 1800s in Australia, and came to be known as the Australian secret ballot. The idea was that the electoral authority would print standardized ballots, and voters would be required to vote by printing standardized markings on the ballot. This simple innovation prevented individuals from exposing their vote by using especially marked ballots, and helped to significantly shield the voter from undue influence and coercion.

The system still had a few vulnerabilities that had to be patched by other means. One of these was the possibility of casting multiple votes by using counterfeit ballots; this risk was not explicitly eliminated by the Australian secret ballot, but the risk was ameliorated by making the government issued ballots hard to counterfeit by using specialized printing techniques such as water-marks.

Another potential attack was known as chaining. The idea was that a corrupt agent could extract an unmarked ballot from the polling place, and marking it with a vote for his preferred candidate. Then, the corrupt agent could offer to buy a person’s vote and instruct that person to deposit the pre-marked ballot in the ballot box and bring back the unmarked ballot. Thus, while the corrupt agent can’t guarantee that the person didn’t spoil the pre-marked ballot, at least he can guarantee that the person didn’t vote for another candidate. However, chaining attacks were rare, because it was relatively easy to catch and prosecute the perpetrators, and if one person broke the chain, it was difficult to get another fresh ballot to restart the chain.

Another important avenue of attack involved doctoring the count. This is not that hard to do when the corrupt agent controls the political establishment. However, there are measures that can be taken to ameliorate this risk. One broad category of measures involve transparency, guaranteeing that each step of the counting allows for independent supervision. The second category is based on competing interests; insuring that any conspiracy must involve individuals with competing interests, such as members of opposing parties.

Another class of attacks for which the Australian secret ballot offers scant protection is composed of attacks aimed at affecting turnout. These often include voter intimidation, confusion and misinformation. An example of this involves spreading rumors that a particular class of voters will suffer some penalty for showing up to vote, for example spreading a rumor that if people have unpaid parking tickets they will be arrested at the polling place, or causing some nuisance around the polling place that draws people away from voting.

Finally, one last category of attacks that falls somewhat outside the scope of analysis involves outright use of force, such as sending armed thugs to steal ballot boxes. While the basic law-and-order framework in the US prevents these types of attacks, they are still common in many parts of the world.

Despite some of these vulnerabilities, paper-based elections can be made very secure. While some attacks are possible, they require very large conspiracies from people with competing interests, so attacks are hard to hide and easy to prosecute.

Electronic voting.

The story with electronic voting is quite different, as many commercial voting systems that have been analyzed contain vulnerabilities that could allow small numbers of individuals to steal large numbers of votes with no possibility of being detected. Before describing some of the vulnerabilities that have been published, I will briefly describe the basic architecture of an electronic voting machine.

As an oversimplification, the voting machines work as follows. First, the machine is loaded with an "election definition" from a memory card. The election definition contains information about who the candidates are for each office and what the offices are. The election definition is loaded into the machine by an operator on the day before the election in the process of readying the machine for election day. On election day, voters are given a smart-card that they insert into the machine and gives them the ability to cast one vote for each office. Once the user casts his vote, the card is returned to the election officer who can reactivate the card so a new voter can vote. Once the election is over, an election officer inserts an "administrator" card into the machine which allows her to print out the election results do a final audit and close the polling place.

Access to the machines is tightly controlled by the manufacturer, making it very difficult to do independent audits on them. However, shortly before the 2006 primary season, an independent watchdog group called "Black Box Voting" bumped into a copy of the source code for a Diebold voting machine. An independent audit of the source code lead by Harry Hursti showed many code vulnerabilities involving buffer overflows and other memory problems.

The audit also discovered that the protocols used by the machine were extremely insecure. For example, the handshake performed by the machine to validate a voting card works something like this:

MACHINE -> What kind of card are you.
CARD-> I am a voter card.
MACHINE -> Are you a real card and are you active.
CARD -> Yes.
Machine allows voter to vote.
MACHINE -> Deactivate yourself.
CARD-> OK.

In other words, it is extremely easy for a malicious card to fool the machine into allowing a person to vote multiple times. The protocol for validating an administrator card is similarly vulnerable, and worked something like this:

MACHINE -> What kind of card are you.
CARD -> I am an admin card.
MACHINE -> What is your PIN.
CARD -> My pin is 1234.
MACHINE -> OK.

In short, the machines lacked even basic security, and were very vulnerable attacks. But that was just the beginning. After all, an attack based on malicious cards that exploited these flimsy protocols could in principle be detected by careful analysis of the machine logs. The biggest problems with the machine would not be discovered until later.

Later in 2006, a group lead by Feldman et. al. was able to gain access to a Diebold machine to do a full analysis of both the hardware and the software. What their group found was that the machines had an automatic update feature, such that if the memory card contained a file called nk.bin, the machine would assume this file was an upgrade to the voting software in the machine. This meant that an attacker could replace the voting software with a malicious version that could easily throw the vote to one of the candidates. Moreover, the malicious software could write malicious nk.bin files to any card that was inserted into the infected machine; if any of this cards was later inserted in a different machine, the new machine would also be compromised, thus allowing the malicious software to spread like a virus.

In general, what many of these studies have found is that security is only a marginal concern in the design of these systems. For example, the systems have no trust boundaries between components, which make for very brittle systems and make them vulnerable to malicious insiders.