E-Voting Synopsis, Group 1

**Summary:** Our readings had to do primarily with the reliability and security considerations of internet voting. It would be fair to say that the crux of our reading dealt with the possibility of an attack on the voting system if e-voting were implemented.

The first thing our reading pointed out is that it’s essentially impossible to determine the likelihood of an attack on any implemented e-voting system; one cannot objectively determine whether or not some hacker will make the attempt to hack an e-voting system. Instead, the authors of our reading (notably Rubin and Wallach) focus on how much effort would be needed to launch a successful e-voting attack.

Wallach’s paper on risk assessment uses a “big-O” notation, which is the theoretical measure of the time and memory needed to solve a problem with the size of $n$ (Definition courtesy of National Institute of Standards and Technology). Restated, big-O is a constant describing the amount of effort needed to accomplish something; in this case, hack America’s hypothetical e-voting system.

Wallach sets up three levels of difficulty/scale: $O(N)$, $O(P)$, and $O(1)$. In $O(N)$, an attack on a precinct would need to target everyone involved in the precinct ($n$: total number). An example would be bribing everyone in a certain precinct to vote for your candidate. $O(P)$ represents targeting only a certain amount of people in the precinct, who represent segments of the precinct’s population. An example of an $O(P)$ attack would be waylaying a postal worker, or bribing an official vote counter in the precinct. Then there’s $O(1)$, “constant”, attacks. The amount of effort you put in for $O(1)$ attacks is a constant; it doesn’t matter how many people there are in the precinct. An example would be a computer virus that affects all e-voting stations within a precinct.

As you may guess from my example, an $O(1)$ attack would be the worst type. The disturbing possibility is that an e-voting system would necessarily be more centralized than our current voting system, thus making it more vulnerable to $O(1)$ attacks. As Wallach concludes, “the constant-effort attacks against internet voting, and the lack of adequate remedies, provide more than sufficient justification to use other modalities for conducting elections.”

Rubin, who also writes on security considerations but more specifically on remote internet voting (voting with one’s computer), continues to underscore the terrifying
potentiality of an attack on an e-voting election. Whereas Wallach favors a statistical analysis of the effort needed to successfully attack, Rubin points out specific possibilities, discussing in his article certain viruses currently in existence that could be easily modified to attack an election. Rubin points out that hackers could easily create fake voting sites, manipulating the voter into believing that he has successfully voted. Rubin also points out that the majority of the potential electorate operate on only a few platforms, such as Netscape Navigator, Internet Explorer, and AOL. Firstly, this puts the election in the hands of a few private companies; even if we trust the companies themselves, we might still be victims of a disgruntled programmer within the company. With remote internet voting, then, we’ve centralized the avenues of voting even more, increasing the feasibility of a $O(1)$ attack. A core theme in Rubin is pointing out that it is essentially incredibly easy for computer-savvy individuals to a. create some type of destructive virus and b. trick non-computer-savvy individuals in a variety of ways. Some alternatives Rubin suggests for mitigating these risks he later dismisses as being too subject to the ‘digital divide’: not everyone has computers, and the security technology that would be needed to help ensure risk-free voting would disenfranchise the electorate even more.

Our other readings consisted of a rundown of the Help America Vote Act, which compels all states to create a directory of registered voters, a comparison between Las Vegas casinos and electronic voting machines, where the state of Nevada has an oversight system on casinos that should be implemented on e-voting machine companies, and a statement on Internet voting prepared by a score of distinguished computer scientists. These scientists provide a list of problems that must be addressed before e-voting can be adopted. Among which is the suggesting that there must be a ‘voter-verified record’ of votes, which dovetails with our final reading (The New York Times) which suggests that electronic voting machines provide a “voter-verifiable paper trail”. Both articles seem to suggest that in times of dispute, the paper record, not the electronic record, be accepted as the ultimate standard of how the vote counts. The conclusion of the computer scientist’s statement is that their statement is not meant to say that there are no current problems with voting, only to bring to attention a list of problems that currently plague e-voting.
**Reflections:** At different points I was struck by how easy it would be to pull off one successful type of attack, and how difficult it would be to pull off a different type of attack. For example, for a O(N) attack, Wallach was at points reduced to saying that hackers would break into people’s homes to tamper into their computers. This is laughable. In fact, I couldn’t see how any proposes O(N) attack was feasible. The numbers are simply too great. Admittedly, you may only need 1,000 people to sway a vote in an election for a particular precinct, but even then it’s not rational to worry about having 1,000 houses broken into.

In fact, a lot of the possibilities for attacks on both traditional and e-voting elections seem to rely on an ‘inside man’, which seems to be an issue of human resources as much as a consideration of technological limitations.

It was Rubin’s article that made me genuinely concerned over the ease of disrupting an e-voting election. Admittedly, Rubin’s article focuses on a subset of e-voting, which is Remote Electronic Voting. But Rubin’s continued casual reference of viruses that already wreak havoc on the Internet underscored the ease by which a major site could be taken down. Again, however, Rubin’s O(N) attacks, such as B02K which takes over another computer, seem farfetched. Not because the technology doesn’t exist, but because a hacker would have to go out of his way to disenfranchise just one voter with B02K. This further cements for me the idea that 0(N) attacks can be all but discounted when calculating the security of internet voting.

I found the comparison between Las Vegas slot machines and electronic voting machines intriguing. I wonder if the comparison is fair, in this sense: Vegas casinos have been around for decades now, while e-voting machines are a relatively new phenomena. Government has had time to measure and set up regulations for gambling. This is not the case for e-voting. Of course, this may be more of an explanation than an excuse; it does not dismiss the necessity for government oversight of e-voting machines.

My conclusion after our reading is, predictably, that much is left to be desired in internet voting. I still think it is a legitimate possibility for the future, however.