Brendan Song

b7song

20466121

CS458 Assignment 1 Milestone

1. Paper-Based Voting

- Interception: possible but not easy in person
    - Intercepting votes to the ballot box would be extremely difficult under the assumption that officials are doing their jobs with some sort of competency.
    - Intercepting physically could also be done by posing as an official or as a courier to gain access to the ballot box. This assumes the attacker can successfully social engineer other people to appear as someone trustworthy and with authorization to the ballot results.
    - Intercepting vote results over the phone would be an easier proposition since a call could be re-routed multiple times to have the hacker on the line just listening.
- Interruption: impossible
    - Voting is not reliant on time as people can vote early or slightly later depending on results revealed so far. Regardless, there are always options for people to vote and it would be extremely difficult for an attacker to prevent votes from occurring. People can even be diverted to other voting stations under extenuating circumstances like weather conditions.
    - The only way an attacker could prevent votes is to physically incapacitate individual voters which is difficult to accomplish on a mass scale.
- Modification: possible but requires co-operation from others
    - Modification is nearly impossible on an individual effort since interception is difficult as is.
    - An attacker could attempt to collude with officials to modify the count of the ballots after voting has completed. However, this requires the full co-operation of all officials and assumes there is no way for additional verification of the votes to be done after the official count.
- Fabrication: possible and most likely to succeed
    - The attacker could create fake identification of residents who have historically not voted or are not likely to vote and pose as them to sway the count. They could also simply pay residents to cast certain votes in person.

Internet-Based Voting

- Interception: possible and most likely to succeed

    - The hacker can easily execute a man in the middle attack over public WiFi spots to observe all traffic that goes through, including votes.
    - The hacker can also set up a fake voting website to handle voting and pass it on to the actual government site after seeing the vote and credentials of the person.
- Interruption: possible but requires poor government infrastructure
    - Assuming the government does not have denial-of-service protection, a hacker could disrupt voting by launching an extended DDoS attack on voting servers. However, this attack would need to be extended for a long duration and requires the government to be incapable of solving the issue.
- Modification: possible but requires an interface illusion
    - This assumes votes are encrypted when they are being transmitted to and from the government servers.
    - If the hacker can gain access to a voter's device, they can ensure specific scripts are run without the user knowing. This would require installation and the user not realizing their device and browser have been modified. The attacker can then inject scripts onto the voting web page and change the user's vote before submitting it to the government. This effectively creates an interface illusion since the user thinks they are voting for a candidate when the script is actually submitting a different vote on the user's behalf.
- Fabrication: possible
    - Since the hacker will only need an authorization code and url to pose as a voter, the hacker could crawl the internet looking for voting urls. They could then brute force the code and make a vote once it has been cracked. However, this would require the voting site to not have anti-brute-force implemented and the hacker would have to make sure they constantly mask their IP address to avoid suspicion.
    - The hacker could also physically gain access to the urls and codes by posing as a courier or having them delivered to their address. This assumes the voters are unaware their mail has been rerouted or interrupted.

2. I feel that privacy is more important since people should have control over their own information. Governments/companies should spend an equal amount on privacy and security since they are both issues in the modern world. Spending more on one or the other results in compromises and reduces the user's trust in the government/company.

Snowden's actions were a security breach since he compromised the existence of the NSA. This means the system can no longer guarantee correct and meaningful results for the government since the public can alter how they interact with technology. I think his actions did ultimately threaten national security since government surveillance could no longer be as heavily relied upon to identify potential threats. I think protecting privacy is justified at the cost of security since people should have a right to controlling information about themselves.

3a. Confidentiality - The doctor is an authorized party but passes the info to an unauthorized party without client consent.
3b. Integrity, Availability - The hacker intercepts requests to websites and alters them to provide the “wrong” data. Also means the sites become unavailable to users on the WiFi network.
3c. Confidentiality, Privacy - The hacker is an unauthorized party but gains access to user info through an authorized party. The user gives the social network their info so they are willingly compromising privacy in the process.
3d. Privacy - The parent is observing the child’s actions without their knowledge/consent. The child is unable to control what the parent sees.
3e. Privacy - The program observes and steals private info of the user. The user is unable to control who gets to see their login info.
3f. Availability - The Internet is no longer accessible by people in the area.

Exploits
1. This exploit takes advantage of the relative pathing submit uses when it wants to make a directory. Rather than providing /bin/mkdir as the path to the command, it simply uses “mkdir” so it will search the current folder before moving on to the bin folder. In my exploit I make a file named “mkdir” and simply run /bin/sh in it to gain root control whenever submit attempts to make a directory. NOTE: submit can run mkdir twice so the user may have to exit twice to go back to the normal user command line.