Armand Nasseri
10/9/19
ECS 153

Homework 1

1) Privacy laws impact system administrators to monitor systems because of the Privacy Act of the United States. The law denotes that unauthorized disclosure of systems would result in jail or fines. In other words, system administrators must have legal authorization to monitor for intrusions.

2)

a) Some PostScript engines allow a user to execute system-level commands that are contained inside the PostScript file. Therefore, an attacker could simply place a deletion command inside this file and cause files to be deleted when a person runs the PostScript engine.

b) To prevent this kind of attack, the system administrators could limit privileges and set up a Janus configuration file to restrict execution of specific programs. If an attacker then tries to run a command that he does not have the privileges for, it will be rejected by the system.

3) In the program I wrote to test the provided functions, I noticed the following problems:

a) There is no size check on put_on_queue() to disallow a user from adding elements that exceed the capacity of the size. Therefore, it will keep allowing unbounded element additions.

b) In take_off_queue() there is no condition to check if the queue is empty and it will allow a user to remove elements that do not exist. In addition, this will allow the queue to keep decreasing size for values < 0.

4) Cryptography alone may not be enough if the developers do not understand the context in which they are using it or if they do not know if it is needed to use it at all. If untrusted or unauthorized users can access a 2 way communication system, then cryptography would not be enough. Other security mechanisms would be necessary for protection in this situation.

5) It is important to preserve the anonymity when a ballot is taken because if it leaked, it may not give true vote preferences. The voting system is structured so that no one can see who a person voted for because someone else could take that ballot and influence another person's voting decision. When it comes to ATM policies, it is important to provide the personal user a receipt of a personal transaction.

6)

a) The weapons worked perfectly during experimentation because they were only tested on a limited amount of scenarios. However, there were many hidden complications and missing requirements that ended up exposing the system to vulnerabilities which compromised the system entirely. As a result, the weapons failed in battle. This applies to

computer security in the sense that we may think our software is flawless, but actual real time scenarios could prove otherwise.

b) The Battle Analyzer failed to take into account the possibility of a massive attack from the enemy even though the intended design should have accounted for that. In computer security, we may think that we have accounted for all cases, but there could still be some weaknesses that cannot be revealed until the system actually fails in practice. Some upgrades may need to be considered in order to have a more reliable system.

c) The flaw of the Exponential Field was that it could never restore the initial state of the ship exactly as it was. It produced many asymmetries and distortions that could be accumulated. The precision ranging equipment was thrown out of adjustment. No single ship could detect this change, but multiple ships communicating to each other could. The enemy ships most likely communicated this information to each other whichNorton failed to account for in his experiments. In regards to computer security, we may believe that we have a great idea to implement in a system, however, there could be hidden consequential problems that could compromise the system as a whole.