Name: Nick Kvigne

CS465 Introduction to Computer Security Homework 3

**3.1** Explain the suitability or unsuitability of the following passwords:

**a.** YK 334 - This is not very good because it is so short

**b.** mfmitm (for “my favorite movie is tender mercies) – this might not be good since it has a personal connection, which could be found on social media or other sites

**c.** Natalie1 – this is not good since it is just the person’s name and one number

**d.** Washington – this is a common word from the dictionary, so not good at all

**e.** Aristotle – this is a name that can easily be guessed, not good at all

**f.** tv9stove - this is using a permutation of simple words, so not very good

**g.** 12345678 – super simple pattern of numbers, this is very bad

**h.** dribgib – this seems to be the best, with what seems to be a random bunch of letters

**3.2** An early attempt to force users to use less predictable passwords involved computer supplied passwords. The passwords were eight characters long and were taken from the character set consisting of lowercase letters and digits. They were generated by a pseudorandom number generator with 215 possible starting values. Using the technology of the time, the time required to search through all character strings of length 8 from a 36-character alphabet was 112 years. Unfortunately, this is not a true reflection of the actual security of the system. Explain the problem.

Once the hacker could figure out the first character of the password, the guessing would only be for 7 characters, taking away all 8 character passwords without that first character. This would keep going until the password was found, much faster than what the system would say it takes.

**3.3** Assume that passwords are selected from four-character combinations of 26 alphabetic characters. Assume that an adversary can attempt passwords at a rate of one per second.

**a.** Assuming no feedback to the adversary until each attempt has been completed, what is the expected time to discover the correct password?

26^4 / 2 = 228488 sec or 63.47 hours

**b.** Assuming feedback to the adversary flagging an error as each incorrect character is entered, what is the expected time to discover the correct password?

Worst case for the hacker would be 26\*4 = 104 seconds but would expect to be more like half of that