**CS 370 Introduction to Security Week 4: Problem Set 4**

Instructor Name: Rakesh Bobba

# Introduction

The purpose of this assignment is to help you gain a better understanding and insight into user authentication concepts and the pros and cons of password-based authentication covered about in Week 4.

Before beginning make sure you have watched the lecture videos on the following and completed the associated practice quizzes.

* User Authentication
* Passwords: Pros and Cons I
* Passwords: Pros and Cons II
* Passwords: Pros and Cons III

Also make sure you have read this week’s assigned reading from the textbook.

# Questions

Please answer the questions below.

## User Authentication and Passwords

Q1[10 pts]: You are designing a password system with randomly selected passwords. The alphabet for the passwords is the set of alphanumeric characters in English both upper and lower case and the integers 0-9.  You are told that the attacker can make 250,000 guesses each minute.

1. If the passwords are 7 characters long, how long until the attacker has a 50% probability of correctly guessing user’s passwords in an offline attack.
2. How long do the passwords need to be to ensure that the 50% success rate is not reached until after 2 years?
3. If the users select their own passwords, does this affect the relevance of your calculations from parts (a) and (b)?  Explain your answer.

Q2 [4 pts]: iPhone 6 includes a fingerprint scanner which the user can choose (not) to use. Do you think activating fingerprint scanning would increase the security of the cellphone? Why or why not?

Q3 [3pts]: Bloom filter is an efficient way to preemptively reject bad passwords with high efficiency, but it has a false positive rate (incorrectly rejecting good passwords). What can you do to decrease the chance of a false positive?

Q4 [3 pts]: Why will a bloom filter never give a false negative (accept a bad password)?

Q5 [3 pts]: It is common practice not to store user’s password in clear text. However, if an attacker has seized control of the password database, he is likely already capable of modifying any user data on the site as an administrator. Why bother hashing the passwords then?

Q6 [3 pts]: It is common practice to salt the user’s password in addition to hashing. What attack does this practice prevent?

Q7 [4pts]: Does a “salt” used in password hashing need to be kept secret? Why or why not? Compare and contrast “salts” and “initialization vectors (IVs)” used in CBC encryption mode.

# Submission Details

Submit a PDF file with the questions and your corresponding answers.

The assignment is worth 30 points. It is due Saturday of Week 4 at Midnight.