EE 8372 CRYPTOGRAPHY & DATA SECURITY

Homework 3
6 February 2020

Professor Dunham
Due: 13 February 2020

Suggested Reading in Menezes, Oorschot and Vanstone: Chapter 10, Sections 1-3 and 5.

1. For a single password authentication system, it is desired that the probability a password be guessed correctly by non-redundant exhaustive testing (*i.e.*, testing each password only once) within 10 days be less that 10^{-4}.

   (a) Letting R be the transmission rate in symbols/second and L be the number of symbols exchanged per password verification, how many distinct passwords N should there be?

   (b) If $R = 2 \times 10^7$ symbols/second, $L = 50$, and the size of the password alphabet is 64 (*i.e.*, number of password symbols and represents base64 encoding used with MIME), how long should the password be?

   (c) Using random password testing, (*i.e.*, choosing each password at random), what is the expected number of trials to successfully find the password?

   (d) Using non-redundant exhaustive testing, what is the expected number of trials to successfully find a password? *Hint:* First show that there are exactly $N!$ ways of performing the non-redundant exhaustive testing where N is the total number of passwords. Hence the probability of any one scheme is $1/N!$.

2. In class, it was mentioned for an optimal password questionnaire where one is only allowed to ask questions of the form “Does X = x?" that

$$\max(2, \frac{n}{\log n})H(X) + 1 \geq E[\sharp Questions]$$

   (a) Evaluate the upper bound when the passwords are uniformly distributed. How close is the bound to the exact expression derived in the problem 1?

   (b) Suppose the passwords are generated as follows. The alphabet of the password consists of six symbols, $0, 1, 2, 3, 4, 5$. Each password is a sequence of 8 letters drawn independently and identically distributed from the password alphabet according to the probability distribution

$$P[X = a] = \begin{cases} 0.35 & a = 0 \\ 0.35 & a = 1 \\ 0.1 & a = 2 \\ 0.1 & a = 3 \\ 0.05 & a = 4 \\ 0.05 & a = 5 \end{cases}.$$

   Evaluate the upper bound on the expected number of questions. *Hint:* Remember for independent random variables that $H(X_1, X_2) = H(X_1) + H(X_2)$.

3. Originally the UNIX operating system used a variation of the Data Encryption Standard (DES) algorithm called crypt(3) to encrypt passwords and stores them in a secure file. Here is a simplified version of crypt(3). A user's key is composed of up to 8 ASCII characters in which the first seven bits of each password character are used. If a shorter number of characters is used, then the trailing characters are fixed as NULL characters. Hence the key size is 56 bits. The key is used to encrypt a message consisting of all NULL characters (all zeros). The output of the DES algorithm consists of 64 bits and is compared to the value stored in the secure password file.

   (a) In the first part of the problem, we consider an exhaustive search attack against a user's password, assuming that we have (legally) obtained access to it. Assume that a dedicated workstation can encrypt 8.5×10^6 passwords per second. Note that specialized systems can encrypt even faster. For the five cases below, determine how many days are needed to search for passwords of length between 5 and 8. Summarize your results in a table and discuss the security implications.

      i. All seven bits are used in the ASCII characters.

      ii. Assuming that a user does not use any control characters, the number of usable ASCII characters becomes 96. *Note:* UNIX in practice does not allow some control characters in a password.

      iii. Assume that only upper case letters, lower case letters and the ten digits are used.

      iv. Assume that only upper and lower case letters are used. *Note:* This is a very common situation.

      v. Assume that only lower case letters are used. *Note:* Some people do not believe in capitalizing anything.

   (b) For the past several years, CPU speeds have double about every 18 months. Discuss the impact of CPU speed improvements for the next decade upon the overall security of the simplified crypt(3) in the light on an exhaustive search attack.