CIS 4360 Introduction to Computer Security

Home Assignment 3, Fall 2010 — WITH ANSWERS

This concerns the basic requirements for Authentiaction and Access Control.

1. The police and the public defender share a computer. What security problems does this present? Do you feel that it is a reasonable cost-saving measure to have all public agencies share the same (set of) computers?
   Answer. A public defender is a public attorney who represents people charged with a crime but who cannot afford to hire a private attorney. The defender's interests in protecting his client may be different from those of the police leading to a conflict of interest, and a confidentiality violation.
   Sharing access to resources among entities with a potential conflict-of-interest is a security threat.

2. A respected computer scientist has said that no computer can ever be made perfectly secure. Why might she have said this?
   Answer. Computers are designed by humans and humans are fallable.

3. Assume that passwords have length six and that all alphanumerical characters, upper and lower case, can be used in their construction. How long will a brute force attack take on average if:

   (a) it takes one tenth of a second to check a password?
   Answer. There are 62 alphanumerical characters, so altogether $62^6 = 56,800,235,584$ passwords. There are $365 \times 24 \times 60 \times 60 \times 10 = 315,360,000$ tenths of a seconds in a year. Dividing we get in the worst case 180 years. On average 90 years.

   (b) it takes a microsecond to check a password?
   Answer. There are $62^6 = 56,800,235,584$ passwords. There are $60 \times 60 \times 10^6 = 3,600,000,000$ microseconds in an hour. Dividing we get, worst case 15.8 hours. On average ~ 8 hours.

4. Assume that you are only allowed to use the 26 characters from the alphabet to construct passwords of length n. Assume further that you are using the same password in two systems A, B, where system A accepts case sensitive passwords but system B does not.

   (a) How many attempts (worst case) are required to guess a password of system A (case sensitive).
   Answer. There are 52 characters so 52^n passwords: 52^n is the worst case number of attempts.

   (b) How many attempts (worst case) are required to guess a password of system B (not case sensitive).
   Answer. There are 26 characters so 26^n passwords: 26^n is the worst case number of attempts.

   (c) Suppose a hacker has succeeded in guessing your password in system B (not case sensitive). How many attempts (worst case) are required by the hacker to guess your password of system A (case sensitive).
   Answer. Each one of the characters is either lower or upper case: guessing the case n times requires 2^n tries. The hacker must make 2^n attempts (worst case).

Mike Burmester