Homework 2

Due: Wednesday, February 5, 1997 at 11:59PM

Analytical

1. A computer security expert claims that one of the measures necessary to obtain computer security is the separation of programmers (who write the programs) and operators (who run the programs once they leave the development phase). Why does this improve security?
2. Modify Anderson's formula to take into account that not all passwords will be the same length. Assume instead that a password is at least one character long.
3. The Morris-Thompson scheme with the *n*-bit random numbers was designed to make it difficult for an intruder to discover a large number of passwords by hashing common strings in advance. Does the scheme also offer protection against an attacker who is trying to guess one particular user's password on his or her machine?
4. Many public key cryptosystems can provide both authenticity and confidentiality. But we usually think of classical (secret key) cryptosystems as providing only confidentiality. How can a classical cryptosystem provide authentication of a user instead of confidentiality of a message?

Programming

5. Write a program to change passwords.The program should prompt the user for his or her current password, validate it, and then request the new password. The program must check that the password is reasonably well-chosen; at a minimum, the password must meet the following criteria:
   a. It cannot be the user's login name or the user's login name reversed;
   b. It cannot be the user's real name (this is stored in the gecos field of the password entry; all names there are of the form *firstname lastname*)
   c. it cannot be an English word (use the spelling checker for this one!)
   d. it must at least 6 characters long, with at least one non-alphanumeric character.

   If the password meets these criteria, it is hashed and the hash is put into the password file. The password file you are to use is ~cs153/hw2/passwd; **do not use the system password file!**
   Hints: You need to get this program working only on the DECStations. Use *putpwent*(3) to write out the password file. For part c, you will need to spawn a subprocess to run *spell*(1), the spelling checker.

Extra Credit

6. Prove that a classical cryptosystem cannot provide both confidentiality of a message and authentication of a user at the same time unless a trusted third party is involved.
7. Think of some other criteria that a good password should meet, and add them to your program.