Protection and Security: Solutions

1. The ACLs are as follows:

File	ACL
PPP-Notes	gmw:RW; *:R
prog1	asw:RWX; *:RX
project.t	asw:RW; users:RW
splash.gif	asw:RW; devel:R

   Assume that * means all.

2. It depends on how long the password is. The alphabet from which passwords is built has 62 symbols. The total search space is $62^5 + 62^6 + 62^7 + 62^8$, which is about 2×10^{14}. If the password is known to be k characters, the search space is reduced to only 62^k. The ratio of these is thus $2 \times 10^{14} / 62^k$. For k from 5 to 8, these values are 242235, 3907, 63, and 1. In other words, learning that the password is only five characters reduces the search space by a factor of 242235 because all the long passwords do not have to be tried. This is a big win. However, learning that it is eight characters does not help much because it means that all the short (easy) passwords can be skipped.

3. Try to calm the assistant. The password encryption algorithm is public. Passwords are encrypted by the login program as soon as they are typed in, and the encrypted password is compared to the entry in the password file.

4. An encryption mechanism requires a way to obtain the original text from the cyphertext using a decryption algorithm and a key. The UNIX mechanism makes use of a one-way function that cannot be inverted.

5. Most viruses do not want to infect a file twice. It might not even work. Therefore it is important to be able to detect the virus in a file to see if it is already infected. All the techniques used to make it hard for antivirus software to detect viruses also make it hard for the virus itself to tell which files have been infected.

6. A worm is a freestanding program that works by itself. A virus is a code fragment that attaches to another program. The worm reproduces by making more copies of the worm program. The virus reproduces by infecting other programs.