Using a Passphrase to Generate a Password

Passwords are notoriously insecure, largely because people select easy to remember passwords to protect their personal computers and their accounts on remote servers. . As well, they often use the same password for all their accounts, because passwords are easily forgotten or not so easily memorized. Many passwords, seemingly secure, can be guessed by crackers through the use of dictionary attacks: you may think syzygy is secure, but a dictionary attack would quickly find it and ...

To create a more secure and relatively easy to remember password, computer security professionals recommend the use of a **pass-phrase**. Simply stated, a pass-phrase can be any easily remembered 10-20 word phrase you desire: a favorite quote, lyrics from a song, lines from a poem, a play or a book. Anything YOU readily remember can be used.

To illustrate, let's use the following: "I think that I shall never see, a bilboard lovely as a tree" (Ogden Nash)

Let's agree that our password must be 10-14 characters long and should – but need not - include a mix of upper- and lower-case letters, numbers and symbols ($@*+%&#). Since our phrase contains only letters, it will be necessary to substitute numbers and symbols for selected characters.

Selecting the first letter of each word of the pass-phrase, we have our prototype password: **IttIsnsablaat.** Definitely not a candidate for a dictionary attack at first glance, although it's still guessable, although not easily, through a brute -force attack. To make things harder for the bad guys, though, let's do a bit of substitution, substituting the number 1 for all letters "I" or "i" and a number 6 for the letter "b". We now have **1tt1snsa6laat** as our candidate password. We have two letters "s", for which we can substitute the dollar sign ($). giving us: **1tt1$n$a6laat**. (If we wish, we can substitute the "@" symbol for the letters "a", which would give us: **1tt1n@bl@@t**.) As you can see, adding symbols makes it a bit more difficult to remember, but remembering the pass-phrase helps in recalling the password. More to the point, however, is that you've now created a password that will be difficult for the bad guys to guess and too time consuming to be easily susceptible to a brute force attack. Remember, the purpose of a password, just as with a lock, is to make it too expensive and time consuming for the bad guys to get at what's being protected.

Using a Passphrase in Place of a Password

A stronger method of protecting important information, whether on your own computer or on the web, is to use a **pass-phrase** in place of a password. Here, the pass-phrase is 4-6 randomly chosen words that include spaces and may include symbols. It's been estimated that a truly random passphrase would take on the order

of 20,000 centuries to guess. There are a number of web sites that will generate passphrases of this type directly on your computer – just google for "passphrase".

The problem here is that a truly random passphrase is difficult to remember. That being so, a slightly less secure alternative is to select pass-phrases as described above, keeping them to 4-6 words, and using them in place of the more commonly used passwords; you may also substitute symbols and numbers to add difficulty. The advantage here is that whatever passphrases you might "create" using this method will be something you're more likely to remember than a truly random string of words. Using the phrase in the earlier example, your pass-phrase would be **I think that I will never** – 6 words with spaces, easily remembered, difficult to guess and expensive to attack.

I'll add in wrapping things up that I do both – strong passwords, created as above, and one or two self-selected passphrases on sensitive accounts.

Bob Melson