Password Lab

Passwords are the most common approach for identifying a user's identity. We use passwords to secure our computers, to send or receive emails or to access special resources. Password guessing has always been the favorite method of cracking into computers or circumventing security measures.

Commonly four methods to guess a password are used:

- Blatantly obvious password such as “Password”, “Superuser”, the account name, one of the preceding spelt backwards, or a blank password.
- The cracker has some personal information about the user. Frequently people use the names of their cats, dogs or spouses as their passwords.
- Monitor manufacturer names, keyboard brands or any word visible from where the user logs in.
- A brute force attack is one in which all possible words of a certain length are attempted until a correct one is found. Crack dictionaries which contain a list of common words and phrases can easily be found on the Internet. Good crack dictionaries contain entire scripts to popular movies and entire sets of song lyrics.

There are a number of suggestions on what you should **not** choose as your password but very few suggestions for choosing **good** passwords. The best password is obtained when the characters of the password are chosen completely at random. This password can be a little difficult to remember. If you force the password to be too difficult to remember users will just write them down and tape them to their monitors.

Here are a few guidelines which can help you in choosing strong, almost random, but easy to remember passwords.

Use Long Passwords

Choose passwords that are as long as allowed by the software. Make your passwords at least 10 or 12 characters long. Short passwords do not leave enough choices to prevent their being guessed by repeated trials. Ideally your password should contain at least one character from each of the following categories:

- upper case letters (ABC)
- lower case letters (abc)
- digits (123)
- Punctuation and other symbols (!$%)

Why use longer passwords, and why mix in many character types? Let’s fill in the following table and see why.

Fill in Table 1 and Table 2 in the appendix.

Use Shocking Nonsense

Shocking nonsense means to make up a short phrase or sentence that is both nonsensical and shocking; that is, it contains grossly obscene, racist, impossible or another extreme mix of ideas. This technique is permissible because the password is never (ideally) revealed to anyone with sensibilities to be offended.
A very weak example is
`Bart Simpson beats up Einstein', or with some mixing of upper and lower case characters, `bartSimpsonBeatsUpEinstein'.
Making up many far more shocking or entertaining examples is left as an exercise for the reader.

Shocking nonsense passwords which are quite long cannot be easily cracked by use of brute force attack.

Use the First Letter of Each Word

Another technique for creating strong passwords is to use the first letter of each word of an easily remembered phrase. For example `Mhall' is formed by taking the first characters of each word in the sentence `Mary had a little lamb'.

This technique can be further strengthened by mixing the password with some digits and punctuations. For example, `M!hal %l'.

An even stronger password can be obtained by typing one key to the left on a standard QWERTY keyboard. The above password after applying this technique becomes `N!gpk%k'.

Conclusions

Choosing a strong password is just a small step in securing your resources. Using the guidelines above will help you choose passwords that are easy to remember, and at the same time strong.

_____
Name

1. Fill in the following table:

Scenario	Available Characters	Total Number Characters	3 Digit Password Total	6 Digit Password Total
Numeric pin	(0-9)	10	10 * 10 * 10 = **1000**	**1,000,000**
Case insensitive alpha	(A-Z or a-z)			
Case sensitive alpha	(A-Z and a-z)			
Case-sensitive alpha and numeric	(A-Z and a-z and 0-9)			
Case-sensitive alpha and numeric and punctuation	(A-Z and a-z and 0-9 and punctuation)			

2. Assuming that a hacker can attempt 25 logins per second, how long will it take to brute force crack (worst case) each of the password types?

Scenario	3 Digit Password Total (from step 1)	3 Digit Brute Force Attack Time (hh:mm:ss)	6 Digit Password Total (from step 1)	6 Digit Brute Force Attack Time (hh:mm:ss)
Numeric pin	1000	**00:00:40**	1,000,000	**11:06:40**
Case insensitive alpha				
Case sensitive alpha				
Case-sensitive alpha and numeric				
Case-sensitive alpha and numeric and punctuation				

3. Create a password using shocking nonsense (keep it clean please):

_____

4. Calculate the brute force attack time for your shocking nonsense password from step 3 assuming 25 login attempts per second:

_____

5. How would you prevent (or limit) the usage of brute force attacks in your login pages?

_____

_____

_____

_____

6. How could you use *Auditing* to help alert system administrators of a brute force attack?

_____

_____

_____

_____

7. Create a password by using the first letter of each word from a phrase from one of Shakespeare's plays.

   Phrase:

   _____

   Password derived from 1st digit of each word in the phrase:

   _____

   Password derived from 1st digit of each word in the phrase, transposing the QWERTY keyboard one letter to the left:

   _____

8. Find a cracking dictionary (text file containing many words) on the web that lists many common words to use for dictionary based attacks.

   URL _____

9. What is the default password for a Linksys WRT54G Router?
   (Hint: http://www.phenoelit-us.org/dpl/dpl.html)

   _____