Hard passwords made easy

Creating strong memorable passwords using mnemonic devices and word lists

John Locke

In the online world, security plays a role in all online activities. Passwords are the most commonly used method to limit access to specific people. In my previous article (http://www.freesoftwaremagazine.com/free_issues/issue_01/passwd_management/) I discussed assessing the relative value of systems protected by passwords, and grouping passwords across locations with similar trustworthiness.

In a nutshell, don't bother creating and remembering strong passwords for low value systems, and certainly don't use the same passwords for low value systems that you use in high value systems.

In this article, I'll discuss how to create a strong password, and how to keep track of all your strong passwords, if you have a definite need to keep more than a couple.

In a nutshell, don't bother creating and remembering strong passwords for low value systems, and certainly don't use the same passwords for low value systems that you use in high value systems

Creating memorable strong passwords

A strong password is made up of several different types of characters, and isn't a name or word in a dictionary. Many systems that require strong passwords will check any password you try to create against a set of rules. These rules often specify a minimum length, and that your password includes characters from at least three of the following four groups:

Tab. 1: Character Groups

Capital Letters	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Lowercase Letters	abcdefghijklmnopqrstuvwxyz
Numbers	1234567890
Symbols	‘~!@#$%^&*()_+=-[]|}{‘;:”/.,<>?

The exact list of allowed symbols vary depending on the system. Some systems allow spaces in passwords, while others don't. A particular system might also have an international character set that includes other letters or characters.

Time after time, people forced to use strong passwords come up with some gobbledygook thing like “v7GT%Xz2.” Leave a computer to generate a password for you, and you could well end up with something like that. And the next thing that happens is they've forgotten it and need to call the administrator for a new one. It's certainly a strong password, but if you can't remember it, and don't store it in a safe place, it's not an effective password.

I suggest using one of three strategies for creating strong

passwords you can remember:

1. Create a password using a mnemonic device
2. Create a password using a word list with some variation
3. Create completely random passwords and store them securely.

Use a mnemonic device

Remember learning about mnemonics? Not Ebonics, that's something different. A mnemonic is a phrase or word to help you remember complicated or otherwise difficult to remember data. For example, ROY G BIV tells me the colors of the rainbow: Red, Orange, Yellow, Green, Blue, Indigo, and Violet - the letters in the name give you the sequence of the colors.

You can make up a phrase to remember a password, or make up a password based on a phrase that means something to you and nobody else

Jesus Christ Made Seattle Under Protest. No, not because there's so many heathen folk running about - this is a local mnemonic for remembering the order of downtown Seattle's streets, from south to north: Jefferson, James, Cherry, Columbia, Marion, Madison, Spring, Seneca, University, Union, Pike, Pine.

You can make up a phrase to remember a password, or make up a password based on a phrase that means something to you and nobody else. For example, our earlier "vhGT%Xz2" could become "Ve haven't Gotten Ten percent Hex sleep, too!" or some similarly silly meaningless phrase. Our brains are capable of easily substituting one symbol for another. I wouldn't trust this phrase for a password I only used occasionally, but for one you use several times a day, you'll remember it in no time.

For less-commonly used passwords, use a phrase with meaning to you, because you'll remember it easier: "Timmy and Tommy were my first dogs" could become "T&Twm1Dgs," which isn't a bad password at all. Remember your puppies and you've got your password.

Use a word list

A dictionary is a list of words. But I've already told you not to use dictionary words, right? Why is another word list okay?

Because you don't use just a single word, and you don't use a word that has personal meaning for you.

As a service provider, I often have to generate passwords for my customers. This is my favorite technique for doing that. You take a carefully generated list of words, and randomly pick two of them. Then you randomly pick a symbol or number to put between them. If it needs to be more secure, you then randomly make a few of the letters uppercase. Suddenly, you have a strong random password such as "rumpus!friar" or "fUngal)selMa." These can sometimes be quite amusing…

You can also add an element of fun to the actual password generation. Diceware.com (`http://diceware.com`) has two different word lists, and a method of randomly choosing words from them: by using regular dice. You scrounge through all those old board games in your closets to come up with 5 dice, roll them twice, and look up the word associated with the numbers you roll. Then you roll two of the dice to determine which number or symbol to put between them. Voila! You've got a reasonably strong password. I've found these passwords to be quite memorable.

Diceware is actually for creating longer passphrases, instead of passwords. A passphrase is used for encryption purposes, whereas a password simply provides access. Passphrases and encryption are a topic for other articles, but the passphrase generation ideas at Diceware make for a great way to generate passwords.

Store passwords securely

If you need to keep track of a bunch of different strong passwords, you have no choice but to record them somewhere. The problem is, where? Certainly not post-it notes attached to your monitor, or the bottom of your keyboard. I need to generate and store different strong passwords for many different clients. I don't want to remember them all, and I'm certainly not going to ask for them over e-mail, which has the security of a postcard.

If you're in this situation, you need a password vault of some kind, an encyrpted system that lists all of your passwords

and keeps them safe and secure. You still need to remember one password: the one that opens the vault.

I use a program on my Palm Pilot that stores all my passwords in an encrypted file. I can see all the accounts I've set up in the main screen, but to get the password, I have to enter the master passphrase first. After 5 minutes, the program automatically "forgets" the passphrase and re-encrypts everything.

I need to generate and store different strong passwords for many different clients. I don't want to remember them all, and I'm certainly not going to ask for them over e-mail, which has the security of a postcard

There are similar programs available for Windows and Pocket PC. You can also use generic encryption technologies like Gnu Privacy Guard (GPG), part of the excellent ()Wt software and provided in every Linux distribution.

Don't store your passwords in a plain text file, a Word document, an Outlook note, or a note in your PDA.

The important point is to think realistically about your risks. If your passwords are in a plain text file on your computer and it gets hijacked by a worm, virus, or attacker, your password file might get compromised without you ever realizing it. PDAs are incredibly easy to steal - you wouldn't want a thief to have instant access to all your passwords.

Password vault software

For Palm: Keyring for Palm OS (`http://gnukeyring.sourceforge.net`) is a great little free program that encrypts the password database to a password. The encryption is weak, but sufficient to protect your password for a few hours - if you lose your Palm, get a new one, restore your database, and change your passwords. The stronger your password, the longer a brute force attack will take. Also check out Strip (`http://www.zetetic.net/solutions/strip/index.html`) for better encryption, though its database is not viewable on your PC.

For Linux: A plug-in for Jpilot (`http://jpilot.org/`) can natively read the database for Keyring for Palm OS. This makes a great harmony: you can view, synchronize, and update passwords on both Linux and the Palm. Again, note that the encryption is weak, meaning the database can be cracked in a matter of 5 hours or so with brute force. That means you should protect your Palm backups, as well as Jpilot.

With these utilities and a better understanding of how to generate strong passwords you can keep your information safe from prying eyes

For Windows: Try Oubliette (`http://oubliette.sourceforge.net/`) or KeePass (`http://keepass.sourceforge.net/`), both are free software password managers for Windows. And here's another: Password Safe (`http://passwordsafe.sourceforge.net/`), developed by a well-known security expert, primarily written for Windows but with compatible versions for PocketPC and Linux available.

For PocketPC: There's a KeePass (`http://doncho.net/kppc/index.php`) version for PocketPC, too.

For Mac users, try Password Gorilla (`http://www.fpx.de/fp/Software/Gorilla`).

With these utilities and a better understanding of how to generate strong passwords you can keep your information safe from prying eyes.

Copyright information

About the author

John Locke is the author of the book *Open Source Solutions for Small Business Problems.* He provides technology strategy and free software implementations for small and growing businesses in the Pacific Northwest through his business, Freelock LLC (`http://www.freelock.com/`).