Memorizing Strong Passwords

Jan 26th, 2014

A Fact of Life

There's really no way around this: whether you take my advice and use password database software to boil down access to your online presence to a single password or go about things another way, there's going to be at least one or two passwords you must memorize. I'm going to offer three good approaches to achieving a very strong password and note their pros and cons. They'll be listed in what I feel is increasing order of difficulty in memorizing:

1. Patchwork
2. Passphrase
3. Muscle Memory

Patchwork Method

The idea here is to combine several of your older weaker shorter passwords to form a new one. This prevents knowledge of any one or even two of your passwords from immediately leading to this one being compromised while offering an easy way to memorize a strong password. The basic steps are:

1. Gather enough old passwords to achieve the desired length (32 at least if strength is the goal) after they're joined by spaces
2. If necessary add punctuation, a capitalization, or a number to improve the password's dictionary
3. Join the old passwords separated by spaces and place any modifications in an easy-to-remember position

For example, suppose some of our older passwords we still have memorized include:

- 123456
- password1

- abc123
- recession

The result might be: `123456 password1 abc123! Recession` which has 34 characters drawn from a strong dictionary and only needs to have three pieces of information memorized — the order, the capital letter, and the punctuation.

I've also used this technique before switching to the easier and better password database approach mentioned at the top and have this to say about it:

Pros

- Extremely easy to form a strong password and memorize it
- Easy to create variants of it if a different length is needed by adding passwords (even if duplicates) or subtracting them

Cons

- Ideally you need to have gone through at least two or three distinct passwords

Pass*phrase* Method

The idea behind a passphrase is to use a sequence of *words* rather than individual *characters* alone to form the password, so "the magical horse leapt over Jupiter" would work. The immediate and clear advantage is it's easy to get a long memorable password, but the basic approach can have some pitfalls; I propose:

1. Form the basic passphrase in whatever manner you like: song lyrics, a book or movie quote, or something nonsensical like above
   - It should be already easy for you to remember
   - It should be relatively obscure, so not a famous phrase that a significant number of people would know
   - It should be quite long — at least 32 characters including spaces but preferably 40 or more
2. Select a few of the letters to be uppercase with the rest lowercase (or the opposite), not necessarily the start of words
3. Select a few numbers and scatter them throughout the phrase
4. For good measure toss some punctuation, say an exclamation mark, here or there
5. Now memorize *where* the special items (steps 2-4) are, and memorize the passphrase

Here's an example of how this technique might evolve a passphrase:

1. He had won the victory over himself. He loved Big Brother.
2. hE had won the victory over himselF. He loved big brother.
3. hE had won8 the victory over1 himselF. He loved big0 brother.
4. `hE had won8 the vict!ory over1 himselF. He loved big0 brother.`

We arrive at 62 characters after starting with a selected phrase that isn't likely to be memorized by any but a very small number of individuals; the locations of 3 uppercase letters, 3 numbers (and what they are), and 1 exclamation point need to be memorized — this amounts to 10 pieces of information plus the passphrase. The important thing is nobody is going to guess this and it'll be quite far up the ladder when it comes to brute force attacks.

Pros

- Easily achieve very long passwords
- Easy to memorize

Cons

- The length benefit may be mitigated by services that enforce shorter passwords

Muscle Memory Method

I find this technique to be the most interesting; the idea is to train your fingers to memorize a password through muscle memory:

1. Generate a random long and strong password from your favorite generator — try this password generator for example; a length of about 23 is satisfactory but a bit longer (say, 32) would be better — you can stitch together two outputs of that generator if this is desired
2. Open up a text editor and copy the password in
3. Looking at the screen, transcribe the password on the next line; repeat this step as often as needed until…
4. Eventually you will start to be able to enter parts of the password without looking at it; focus on getting those parts right as they come and once mastered move on to others
5. Once you can type the entire password consistently without looking, keep doing it for at least five minutes straight — longer if possible
6. Repeat the password one more time and print that one lone line or save it somewhere inconspicuous
7. Over the coming days start using that password; if you resort to the backup repeat the transcription exercise a bit

I've done this, and while I might be a bit unhinged and/or paranoid this is what I have to say about it:

Pros

- Depending on how your mind works, there's a chance that by memorizing the password this way you will find yourself unable to write it down on paper or recite it in your head. This is the ideal outcome; it means only your fingers 'remember' it through muscle memory. This means you cannot divulge the password if strapped to a chair and beaten with a wrench; of course, you'll probably give up the fact you can provide the password if given a keyboard, but it's still a fun thought.
- Because of the way this password was memorized, you should be really fast at typing it!
- As it's properly random there's not the slightest chance of another human guessing it (of course this has nothing to do with brute forcing it with a machine)

Cons

- I figure this probably won't work for some people just because of the differences in the way many of our minds work
- The longer the password, the harder it is to learn

Memorizing Long Passwords Safely

In case you're new to the world of learning longer passwords, consider this advice. Once you've formed the password print out a backup copy of the password or save a text file containing it somewhere inconspicuous then use it for a week and only use the backup copy if necessary. Once you're comfortable enough to go without it, securely delete the backup. If you made a print out either shred it or (safely) burn it. If you saved it to your computer then securely delete it:

- Linux: `shred -vuzn 7 /path/to/file`
- OS X: `srm -i -m -z /path/to/file`
- Windows options (I haven't tested these)

Yes, it’s unlikely for this level of precaution to be necessary but it’s mostly about the principle of what you’re doing: why bother with a strong password if you’re not going to cover every base security-wise?

Conclusion

All of these approaches should be more than adequate for generating and memorizing a very strong password that will stand up to basic brute force attacks (at least for a while, and almost certainly better than 99.99% of other passwords in use). For my purposes I’m using a strong password based on the patchwork method where the constituent passwords were originally memorized from the muscle memory method for my password databases (as mentioned at the top of the article), and I feel very secure.

Again, while these methods may seem like paranoid overkill it comes down to this from my perspective: by using the password database approach I can have access to every credential in a strongly secured database where only a few passwords need to be memorized and never written down. So why not jump through a few hoops to make one of the critical pieces of information highly secure? Even though I feel being attacked is very unlikely, if I am I won’t be worried about anything — that peace of mind is worth it to me.

Posted by Isaac Velando Jan 26th, 2014 infosec, passwords

Tweet 1 1

Comments

1 Comment **greplinux** **Login**

Sort by Best **Share** **Favorite**

Join the discussion…

Carter Connors · 12 days ago

HintCard method - Use one secretline for HintCard and remember two symbols as a start point. Your pass will be complex. All my 1k passwords are complex but I can't forget them. They are written on one card 86x54. I KCCO.
See more HintCards.info

| · Reply · Share ›

ALSO ON GREPLINUX

What's this?

Recent Posts

- What's Different About Linux: Programs
- Account Password Security: Advanced Edition
- Not Just the NSA: Privacy Breaches Closer to Home
- Password Security Failure: When Websites Don't Get It
- The @N Hack: Why Absolute Security is a Myth

GitHub Repos

- twitter-blog-broadcaster

  A Twitter bot written in Python meant to broadcast a site's blog posts or similar resources through nicely hashtagged posts (not designed to be followed)

- dotfiles-general

  A collection of assorted dotfiles not directly tied to the desktop environment or window manager

- btrfs-backup-scripts

  A collection of scripts intended for both periodic and manual use for creating backups with a btrfs filesystem

@iwvelando on GitHub