Online Hygiene:

Safe Password Practices

Maxwell Memorial Library's Technology Class
Thursday, May 23, 2019

0. Introduction

Contrary to the Hollywood depiction, most computer hacks don't come about because some super-genius finds a way to crack a database of encrypted passwords. Cracking strong encryption is a very time consuming process, but guessing what someone's weak password is might be fairly easy.

You undoubtedly know not to use 11111111 or your birthdate as a password. You probably know to use a combination of digits, special symbols, upper-case letters, and lower-case letters (many sites require this). But there are probably at least a few sites that you use the same password for, and it might be the case that you carry a written list of your passwords with you.

Today's Tech Program presents some techniques and tools for coming up with safe passwords, for safely having them at your fingertips when you need them, and for added security beyond good password practices.

1. Basic ideas in safe password management

A good way to think about passwords is to view them as the keys or combinations to the locks on your various online "boxes." In this analogy, some "boxes" are like safes. These are the accounts that you're willing to put some real effort into keeping secure (for example, your financial accounts). You would like these passwords to be unique[1] and effectively uncrackable, and you probably wouldn't walk around daily with these passwords in your wallet. On the other hand, though, just as you want to be able to find your safe deposit key when needed, you don't want to forget them. So you'd like some system that makes it easy for you to remember them and virtually impossible for anyone else to guess them.

1 Ideally, you'd like them to be completely unique in that they are strings that aren't already used by anyone for anything. More realistically, you'd like them to be unique at least within the set of all of your own passwords.

Continuing with the analogy, other "boxes" are more like your house or car (for instance, email, social media, and so on): you don't want anyone cracking these accounts any more than you want them cracking your financial accounts, but you might need to have access to these passwords frequently and easily. Just like your car or house keys, then, you'd like to "carry" them with you everywhere.

This is where the analogy starts to break. Because if you carry your passwords in the same way as your car and house keys (as physical items in your bag or pocket), it's not the same as carrying physical keys. It's more like carrying the keys and a key duplicating machine that will make perfect copies. If someone sees your house key, you're still pretty safe from being burglarized; if someone sees your password, they now *have* your password.

So how do you create safe passwords that you can remember without writing them down? We'll talk about methods in a bit, but first consider the properties we want passwords to have:

1. Easy to remember

   Many OCPL patrons use their birthdate or part of their phone number as the PIN for their library cards. This would be a bad choice for any password that needed to be at all secure. However, since there is little incentive for bad actors to crack your library account, these patrons find that the ease of remembering the PIN is more important to them than making sure it stays secret.

   To push a bit on the analogy above, some accounts are like luggage with a cheap luggage lock: sure, a really good password would be the most secure way to go, but is it worth the bother?

2. "Uncrackable"

   I've put scare-quotes around the word *uncrackable* since absolute uncrackability is an impossible requirement. However, the more random a string of characters is, the harder it is to guess, and the longer it will take a computer to crack it.[2]

   The word *random* in the previous paragraph is important. If we could actually remember arbitrary strings of characters, the ideal way to come up with passwords would be to roll a 95-sided die (1 face for each character on a standard keyboard) multiple times and use the resulting string. Given reality, though, see item (1) above.

3. Hard to guess

   This is where those security questions like "What was the name of the street you grew up on?" are coming from. Personal details that are not easily accessed, obscure hobbies, and other things about you that are off the beaten path can make good sources for material to use in passwords.

2 Longer is better and more random is better. The combination of length and randomness is more or less what is meant by *entropy* in the *xkcd* comic I use below.

4. Fresh

   None of your accounts should have the same password for long stretches of time. A saying among tech-types is that passwords are like underwear: they shouldn't be shared, and they should be changed regularly.

   In particular, if you have an account with a provider who's system got hacked, change your password with them as soon as you can.

5. Unique

   Ideally, none of your accounts use the same password. There are at least 2 reasons for this ideal:

   a. Most importantly, if someone gets a hold of 1 of your passwords, then only 1 of your accounts is placed at risk.

   b. From the standpoint of public cyberhealth, as it were, the more duplication there is in a site's encrypted password database, the easier it is to crack if it falls into the wrong hands.

As you can see (and as you have no doubt experienced), these ideals contradict one another. We'll now look at some methods people have come up with in order to craft workable compromises among the ideals.

2. Password management techniques

2.1. Words but with upper, lower, symbol, digit

When you're creating or changing a password, many sites require you to use a string with at least 8 characters which has characters from each of the 4 classes of the lower-case Latin alphabet, the upper-case Latin alphabet, the digits from 0 to 9, and some designated subset of the other 33 characters on the ASCII keyboard (the "special characters"). The purpose of this requirement is to force greater randomness than users might come up with on their own. As the first row of the comic below illustrates, however, the ideal of trying to keep one's passwords relatively easy to remember can get in the way of actually achieving.

Read the comic below in Illustration 1. Now let's look at the first password — **Tr0ub4dor&3** — in some detail and see how it might be enhanced:

1. ✓The word chosen to work from is obscure.

   While even obscure dictionary words shouldn't be used without some sort of transformation first, obscurity does help with keeping passwords harder to guess. This is where off-beat hobbies and interests can be useful.

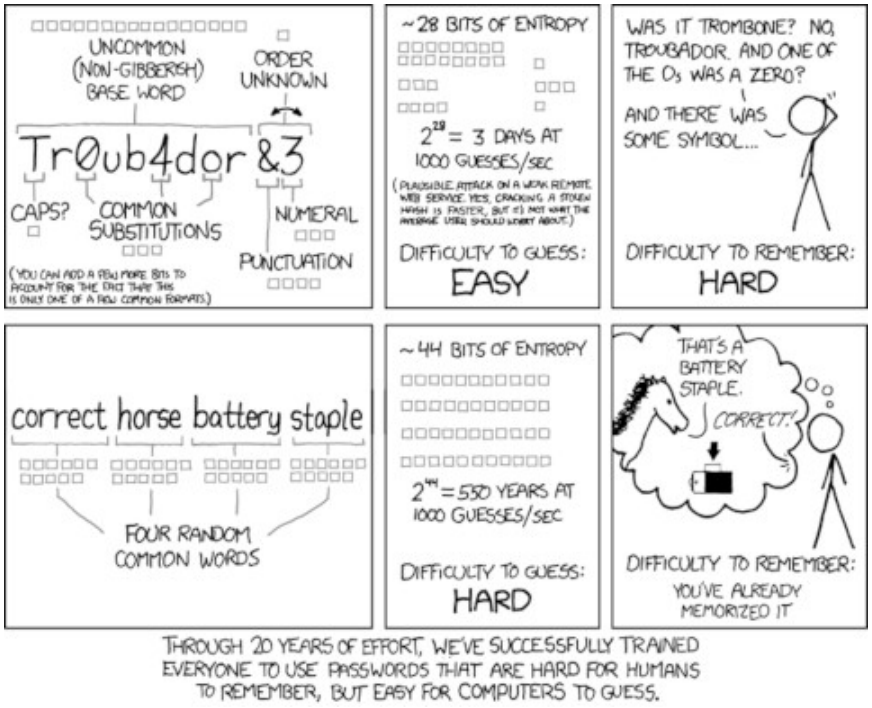

Illustration 1: xkcd #936, "Password Strength"
License:CC BY-NC 2.5

2. ¿? The single upper-case letter in the string is used at the beginning.

   Very often, people will capitalize the first letter in their string and leave all other letters in lower-case. In a completely random string drawn from the 92 characters that you might be able to use, you'd only expect a upper-case letter in the first position between a quarter and a third of the time.[3]

   This is by no means fatal, however, and the slight loss in security from always using capitals in the first position would be more than overcome by using additional characters. However, …

3. ¿? The string could be longer.

   At 11 characters, it certainly meets the requirement of 8 or more characters, but many of my sources are recommending 12 characters or more.

4. ✗ The substitutions are obvious.

3 The string here has 11 characters, so (again assuming a uniform, random distribution of 92 symbols) we'd expect about 3 upper-case letters, 3 lower-case letters, 1 digit, and 3 or 4 "special characters."

I would assume that any software being used to guess passwords would supplement its dictionary with all the strings that substitute '0' for 'o/O', '1' for either 'i/I' or 'l/L', '3' for 'e/E', '4' for 'a/A', and so on. This password doesn't have obvious special symbol substitutions, but I'd also expect that substitutions like '@' for 'a/A', '$' for 's/S', and so on would also be weak.

5. ¿? The word being worked from is misspelled, but the misspelling is a common one.

   An uncommon misspelling can be a good idea (if it's one that you'll remember you used), but common misspellings might be in lists that crackers use.

One way to avoid dictionary words, even obscure ones, is to start instead with a phrase or sentence that means something to you and is "fixed" (that is, you never express the phrase in different words). You then reduce the phrase or sentence down to the first letter of each of its words and the first digit of each of its numbers.

As an example, suppose you have noticed that whenever you're thinking about where your grandmother grew up, you express it as "My grandmother was born in Oakland, California in 1895, and she graduated from Berkeley in 1916." The potential password would be **MgwbiOCi1asgfBi1**.[4]

I would tweak this string a bit, though, before using it. First, it doesn't have any special symbols. Even though this starting string is not a word at all, obvious substitutions are still not the best thing. However, the string's length (16 characters) and seeming randomness may mean that we can use 1 such substitution safely. I'll change the 'g' from *graduated* to an '&':[5] **MgwbiOCi1as&fBi1**.

Another change I'd make is to drop the century from the years in the string and use '95' and '16', respectively. This is because it is a bad idea in general to have parts of the string correlate strongly with each other. In particular, using 2 terms in the string that necessarily repeat characters makes it more likely that traces of the repetition will remain even after encryption.[6] The string is now **MgwbiOCi9as&fBi1**.

We could stop here since don't necessarily have to do anything about the upper-case 'M' at the beginning. As mentioned in the analysis of the *xkcd* strip, we expect an upper-case letter here about a quarter to a third of the time. On the other hand, this particular base-sentence gives us an

4 For my purposes, the period at the end of the sentence is not part of the password string. I would tend to leave end punctuation off of a password — at least off of its final position — since that's a position where it might be expected.

5 This is a slight sacrifice of security for memorability, and you want to keep from making too many such sacrifices within a given password. The longer your starting phrase, though, the more wiggle room you have.

6 Of course there is a fairly strong correlation between one's year of birth and one's year of graduation from college, but unless a hacker has reason to believe that the database they hacked has a sufficiently large number of passwords that were generated using birth and college graduation dates for various individuals, it seems unlikely to me that they'd look for the traces that the correlation would leave on the encrypted data.

opportunity to easily shift the capital over to *Grandmother* (clearly, that's her name, right? :-)): **mGwbiOCi9as&fBi1**.

For more ideas on how to generate strings like this, see the articles listed at the end of the handout.

2.2. Password managers

One way around the problem of generating passwords, remembering them, and keeping them fresh is to use a password manager. A password manager is an application that is effectively like the computerized version of carrying a piece of paper with all your passwords but with more security to it and with more capabilities. Storing all your passwords in plain, unencrypted text on your computer or on a USB stick would be a bad idea since anyone who got a hold of the file would have all your passwords without any further effort. The manager encrypts your data, though, so it is secure.

As an aside (but an important one), I should mention here that if you have your internet browser (for example, Chrome, Edge, or Firefox) remember your passwords, you probably do have your passwords stored on your computer as unencrypted text.[7]

Most password manager apps store your data on their servers, making it available on all your devices. Storing all that personal data does make those servers attractive targets for hackers, however, so you want to be sure that the company making the app is taking security seriously.

Password managers are not just a secure means of storing your passwords and giving you access to them wherever you go. Some apps can also generate near-random strings as passwords, taking care of the problems of coming up with secure passwords. Another feature is alerting you to when a site you have an account with has been hacked so that you can change your password with it quickly. Also, some offer wizards that help you with determining your overall password "health" — which passwords you currently have are weak or are duplicates — so that you can work on strengthening at least the more important ones.

Below are some password managers that get recommended often. Note that you should download any password management software directly from an official site since hackers have been known to distribute rogue versions.[8]

- Dashlane (https://www.dashlane.com/)
- LastPass (https://www.lastpass.com/)
- KeePass (https://keepass.info/)

7 Firefox's settings can be changed such that the file will be encrypted. That setting reduces the security risk from having Firefox store your passwords, but it doesn't give you the additional features of a password manager.

8 This is particularly true for KeePass since it is open source. While open source software has security advantages over proprietary software in that its code is open to inspection by the community of experts, its free distribution status means that you have to be sure that your source for an open source app is trustworthy.

3. Articles and webpages with more information

Bojana Dobran, “9 Strong Password Ideas For Greater Protection,” PhoenixNAP (blog), PhoenixNAP Global IT Services, September 29, 2018, https://phoenixnap.com/blog/strong-great-password-ideas

Charlotte Empey, "How to create a strong password," Avast (blog), Avast, August 15, 2018, https://blog.avast.com/strong-password-ideas

Hoffman, Chris. How to Create a Strong Password (and Remember It). How-To Geek. May 29, 2015. Updated May 9, 2018. https://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/

“How Do I Create a Strong and Unique Password?” Webroot: Smarter Cybersecurity. Accessed May 19, 2019. https://www.webroot.com/us/en/resources/tips-articles/how-do-i-create-a-strong-password