Choosing Good Passwords

Introduction

This document presents a plain-language guide to security threats posed by password cracking software, and how to apply good password rules to prevent security compromises. It also gives suggestions for choosing good passwords and making them secure and hard to guess.

The Password Management Problem

It's that time again. You've been asked to change the password that gives you access to all your crucial systems and information. Or perhaps you need to enter yet another new password to access yet another application, document, or system.

Choosing Hard to Guess Passwords

It's tempting to pick something easy to remember, like spelling your user name backwards, or child's name, or a word from the dictionary. The problem is, the easier it is to remember, the easier it is for an intruder to steal.

Malicious intruders often gain access to a company's systems by stealing, or cracking, a password and account name, then posing as that user. If the intruder knows you, they can easily gain access by trying password combinations related to your family or hobbies. If they have physical access to your desk or digital assistant, their chances of getting into your accounts are even greater if you've used something personal for your password.

Hackers use readily available software to rapidly enter random dictionary words until they hit pay dirt, and it can take only minutes! The shorter the password, the faster it can be guessed. Even words spelled backwards, rearranged, or including numbers are not safe. A common misconception is that substitutions, such as replacing the letter l or i with the digit 1 will fool password cracking software. Password cracking programs are smart enough to do this too.

Examples of bad passwords include:

```
mydog2
bi1lsmith
yromem (memory backwards)
win4me
```

The safest solution for choosing good passwords is to use a randomly generated or seemingly random password that:

- Use a minimum password length of 12 to 14 characters if permitted.
- Include lowercase and uppercase alphabetic characters, numbers and symbols if permitted.
- Generate passwords randomly where feasible.
- Avoid using the same password twice (e.g., across multiple user accounts and/or software

systems).
- Avoid character repetition, keyboard patterns, dictionary words, letter or number sequences, usernames, relative or pet names, romantic links (current or past) and biographical information (e.g., ID numbers, ancestors' names or dates).
- Avoid using information that is or might become publicly associated with the user or the account.
- Avoid using information that the user's colleagues and/or acquaintances might know to be associated with the user.
- Do not use passwords which consist wholly of any simple combination of the aforementioned weak components.

Diceware

We also recommend Diceware for generating strong passphrases; easier to remember, easier to type (especially on mobile keyboards) and generally stronger than 8-random-character passwords. It is very important that the words are selected randomly, not taken out of a book or something. We prefer six- or seven-word passphrases. Users are now using ssh keys, and Diceware is great at generating long passphrases that get typed once upon starting up a keyring/session manager.

Writing Down Passwords

If you have too many passwords, it is tempting to write them down – after all, can you really remember 10 different passwords, that change at different times, some of which are rarely used?

Writing down passwords is a serious breach of security, because it means that anyone who can physically get to the piece of paper, sticky note or PDA that contains the password, can also log into systems with your accounts. Should a visiting vendor really be able to sign into the finance application? Should the janitor be able to read your mail?

A better solution is to create a single, strong password, and apply it to all of your login accounts. One password is easier to remember, and is more secure than a post-it note.

Password remembering tools

There are tools that can store passwords for you, making them accessible by only remembering one 'master' password. In these tools you can store system access passwords, web-page passwords, etc. A reliable tool is KeePass which works on almost all OSes. This tool also checks the strongness of user-chosen passwords, or it can provide a strong password for you (and remember it).

Reusing Passwords

Another temptation, when imagination fails, is to reuse old password values when the time comes to change your password. This is also a security problem, since the whole point of a regular password change is to limit the time available to an intruder to crack your password. If an old password is reused, intruders would have more time to crack them. If the old password was already compromised, the new one will compromise your security again.

If you cannot think of a new, secure password – have a program, like Hitachi ID Password Manager (formerly P-Synch), randomly generate one for you.

How to Choose a Good Password

Some security experts recommend using a password based on a mnemonic, such as an easily remembered phrase. For example, take the first letter of a each word in a phrase, then add a few special characters or numbers to it. For example, “lend me your ears” can become “lmye4%”. “To be or not to be, that is the question” can become “2Bor!2b?”.

This is good technique, but you may need some patience to think up a new phrase every time you change your password – especially if you have to think of a different password for every system that you log into. This may lead some users to recycle some version of their old password - another security threat.

Another easy way to choose a good, safe password is to let an application like Password Manager do it for you. Password Manager makes remembering passwords easy by synchronizing passwords, so that you only have one password to remember, and that password works on every system.

Password Manager can provide a suggested list of randomly generated passwords, and reject passwords that do not comply with strong password rules, so that you always choose good passwords.

When to Change Your Password

Perhaps just as important as how to choose a new password is when to do it. New passwords are most easily remembered if you start using them immediately, and use them often. Don't change your password at the end of the day, the end of the week, or before a holiday. Instead, change your password in the morning, at the start of the week. Your mind will be clearer, and frequent use of the new password will reinforce your memory.