MANUAL ON SECURE PASSWORD HANDLING

Version 1.0 EN Patrick Brunswyck

a manual by

all2all

Moving Art Studio a.s.b.l.

Table of Contents

Secure passwords

A 100% secure password does not exist. All passwords have a certain degree of weakness, more or less in comparison with the number of precautions taken by the one who chose the password.

In practice

People have the tendency to easily forget things that are not directly related to their immediate reality. Maybe that is why so many people use easily to guess or hackable passwords to secure data that is not supposed to be seen or used by others. The precautions that will follow are applicable on the every use of a password, independent of whether it involves a password to secure text in a secret file, a login to log on to a forum, to log on to your Unix account, to log on to a Windows 200x machine on the office floor or a password to transfer money on your banking account.

In all these cases passwords are being used to provide access to information for authorised people and to keep unauthorised people at bay. If your password is being used without you knowing it can have numerous unpleasant consequences: financial loss, loss of data, loss of confidential information and so go on.

Dictionary attacks

All words that can be found in a dictionary are a risk, independent of the fact whether or not it is the language that you use. English words or words in your native language (when known) are of course a whole lot more susceptible than if you were to use words in Swahili. On the internet you can find specialised dictionaries to find passwords for a certain application in order to “brute force” attack it, meaning trying out passwords one by one.

Even if you can create a certain level of security by using lowercase with uppercase letters (if possible), than this still isn't a real handicap for these kind of attacks. Also words like “CinDERella” can be found after a certain amount of time.

An English dictionary contains around 150000 words. If you apply a lowercase – uppercase combination on it, you get around 15 million words. Only a few seconds are needed to find the password using the “brute-force” method.

In 2002 a list of 10000 accounts on an operational server were analysed. After 30 minutes a whopping 30% of the passwords were already discovered. (see Passwords: the weakest link?)

Personal data

Keep in mind that passwords based on personal information (names, first names, date of birth, telephone number, movie- or bookcharacters, hobbies or passions of a user, his colleagues, family etc.) are even weaker than those that come out of a dictionary. These passwords can easily be guessed.

In a study executed in 2001 with 1200 English employees, it was discovered that half of them used their name, names of their pets or names of their family as their password. Others used names of their fiction heroes such as Darth Vader or Homer Simpson (see Homeland Insecurity).

Series of letters

Other commonly used passwords are those with a series of letters such as “azerty”,”qwerty” or “12345”, that can be typed very quickly. These passwords are very known, thus, very vulnerable. (there are even dictionaries that focus on series of letters)

“Brute force” attacks

Modern day computers are very powerful. Now systems are available that can easily try out tens of millions of pass phrases a second. For example, the RC5 coding algorithm (considered rather weak). If you compare this number with the number of passwords that consist out of 6 signs (including lower and uppercase characters) you can easily calculate the amount of time needed to “brute force” these passwords.

52 possible characters to the 6th degree (length of the password) = around 20 billion combinations

20 billion / 10 million = 2.000 seconds = around a half an hour.

2 conclusions can be drawn out of this calculation:

- short passwords are weak
- passwords that consist out of a limited selection of characters (only numbers or small characters) are a lot weaker than those that consist out of a larger collection (uppercase characters, numbers, lowercase characters, special characters).

Conclusion

Summarized: passwords need to meet certain complexity requirements for them to offer an acceptable security:

- The passwords need to be long (at the very least 8 characters)
- The passwords may make no sense at all

The following methods can help you find passwords that have an adequate safety and can be remembered fairly easily in comparison with a complete random series of signs:

- Connecting two words (by mixing up uppercase characters and lowercase characters) with a special sign
  (e.g. “4aT&hOme”,"b1G#seCreT", "zEIt+f0rM")
- Using the first letters of a sentence along with special signs and numbers
  (e.g. “"Spau2rP!" for "Some people are unable to remember passwords!")
- Using meaningless words that contain unpronounceable parts combined with special signs and numbers
  (e.g. "dOsil?Ar0n")

❗ Do not use these examples, invent your own!

Why even these precautions are insufficient

Complicated passwords are harder to remember compared to the simple ones. Even if it is difficult to resist the temptation to write them down somewhere, it is far better for you to know your passwords only by memory. Even if you have chosen your password very precariously, others will not save themselves the trouble to try and read it off your screen by means of “shouldersurfing”, via a camera or more extreme, using a keyboard logger that can register every key you have pressed. (So don't check your e-mail on a computer that belongs to people you don't trust).

Another good way to render passwords insecure is by using them for different accounts. If one administrator knows the password of your forum account, he could try these on all of your accounts and hope for the 'best'. That is why passwords shouldn't be used more than a few times and should be changed in regular intervals.

Keep in mind that sometimes passwords travel over the local network of your organisation and / or the internet in clear text form and can be intercepted everywhere on the network. Never use those kind of passwords more than once if you need to use it this way.

It is advisable not to trust anyone when it comes to passwords. Do not hand over a password to a friend (because you might be afraid you will forget it) or because you want to share certain data with someone.

Versions

Version number	Modifications	Author
1.0 NL	Original version	Frédéric Jadoul
1.0 FR	Traduction	Frédéric Jadoul
1.0 EN	Translation pdf NL-> odt EN	Patrick Brunswyck

page	**Modifications**
first	Added Cover all2all GNU Free Documentation License
last	Versions and Modifications
4	Warning sign in table