A simple technique for choosing and managing secure passwords: passwords with a random on-paper part

Alexei Vernitski

1 Introduction

Recently I proposed a novel way of choosing and managing passwords in a secure way, especially suitable for the typical situation of a modern user with multiple accounts and frequent password changes on some of the accounts. The name I suggested for it is 'passwords with a random on-paper part', shortened as PROPP. The PROPP method is also suitable for scenarios in which the user needs to log in on a wide and unpredictable range of devices, although in the description below I concentrate on a one-computer scenario.

2 Using the new method

The rules described in this section are extremely simple – this is intentional. The rules are designed in the way which can be directly applied by a wide range of the users of IT.

Choosing a password

When you choose your password, choose one which consists of two parts. The first part should be a truly random string consisting of five lower case letters. The second part of your password should consist of two randomly chosen dictionary words. For example, your password can be 'qzyotbeanzebra'; here 'qzyot' is a random five-letter string, 'bean' is a randomly chosen word and 'zebra' is a randomly chosen word.

How can you choose five random letters? For instance, if you know how to use Excel, you can use the function =CHAR(RANDBETWEEN(97,122)) to generate a random letter. If you cannot use a computer to generate random letters, opening a book at a random page and choosing the first letters of five consecutive lines is acceptable, but not as good as choosing random letters with a computer.

Managing a password

The random part of your password is not memorisable. Therefore, do write it down and keep it by your computer. Thus, using the example above, you can have a sticker saying 'qzyot' on your computer.

As to the word-based part of your password, it can be easily memorised; memorise it and do not write it down.

You may make it publicly known that you use the PROPP method; this will not make your password insecure.

Managing several passwords

Suppose you have multiple accounts (for example, email, Facebook, etc.). It is good practice to have a separate password for each. In this case, the PROPP method should be used as follows: generate a distinct random part for each account's password (and write them all down, as recommended above); however, the word-based part may be the same for all your accounts (and it should be memorised).

For example, your email password can be 'qzyotbeanzebra'and your Facebook password can be 'zwasrbeanzebra'. Write down the parts 'qzyot' and 'zwasr', noting that these are your passwords for email and Facebook. However, do not write down the part 'beanzebra'.

3 Why is this secure?

The analysis of the security of PROPP needs to be based on a refined classification of attack scenarios. There are some attacks which defeat the PROPP security; however, it is possible to show that these attacks are simply too strong for password security in general and would also be effective against any other method of choosing passwords. There are some realistic attacks which involve the attacker trying to guess the user's password; it is possible to show that PROPP resists such attacks well. At last, there are some unrealistic attack scenarios which assume that the attacker has access to too many technical resources; such attacks would be successful against PROPP, but it can be argued that such a powerful attacker would be able to get the user's password anyway.

Realistic scenarios which are too bad for any passwords

There are situations when attackers steal your password (for example, using a 'spyware' program they install on your computer). In this extremely bad situation, PROPP passwords are as vulnerable (but not less vulnerable) than passwords chosen with any other method of choosing passwords.

Realistic scenarios which do not topple PROPP

Unless attackers steal your password, there are two scenarios in which they may try to guess your password. These types of attackers may be referred to as 'high-tech outsiders' and 'hands-on insiders'.

Sometimes attackers, acting remotely, steal your encrypted password from a server computer. Then they will try to find a password which matches the stolen encrypted password. Such attackers do not have access to the random part of your password which you have written down on paper. Guessing the letters in the random part of your password will take a long time, even with the use of modern computers (see Section 5 for a more detailed discussion).

Other attackers may gain physical access to your computer; they will find the random part of your password which you have written down, but they will not know the word-based part of your password. Guessing the words in the word-based part of your password will take a long time, because such attackers will have to make guesses and enter them into the computer one after another at a relatively slow speed.

Unrealistic scenarios

In theory, one can consider how the previous two scenarios can be combined, that is, attackers would obtain your encrypted password and, at the same time, find the random part of your password. Such an attack would be successful against PROPP. However, it is unrealistic for one attacker both to gain a physical access to your computer and to steal your encrypted password from a server. On the other hand, if this combined scenario occurred then the careful choice of passwords would not help: indeed, this kind of attacker could do such things as install spyware on the user's computer or hide a video camera above it. Therefore, this scenario would require other types of security, in addition to passwords.

Here is another scenario. Suppose the user has accounts in several social networks, say, Acebook, Basebook etc. Suppose that Acebook stores passwords unencrypted (which is an extremely bad practise), and these passwords are stolen by attackers; then, of course, all these passwords are compromised. At the same time, these attackers steal encrypted passwords from Basebook. Since the attackers knows the user's password in Acebook, they know the word-based part of the user's password, which is, according to the PROPP method, the same as the word-based part of the user's password in Basebook. When they try to guess the user's password in Basebook, knowing the word-based part of the password is of some help to the attackers. How can we analyse this attack scenario? It is relatively unrealistic because it assumes stealing passwords from two unrelated servers, and also that one of them the passwords are not encrypted. Even if this unlikely coincidence occurs, the PROPP passwords is still not immediately compromised, since most of the PROPP resistance against an attack on an encrypted password is based on the random part of the password, and not on the word-based part.

Here is one more scenario. Suppose you have decided, contrary to the advice above, to store random parts of your passwords in a file in your computer, instead of writing them on paper. If attackers steal both your encrypted password from the server and the file with the random part of your password from your computer, they will be able to guess your password quickly. However, these must be very powerful attackers: if they have access to files on your computer, probably they can also do such things as install spyware on your computer to steal your passwords and other data. Therefore, this scenario would require other types of security, in addition to passwords. In any case, this scenario would not occur if you stored random parts of your passwords on paper.

4 Why is this convenient?

There are various ways of choosing a good password. For example, many people use phrase-based passwords. Say, your favourite song is 'When Phoebus first did Daphne love'; then by taking the first letter of each word in this line and using a couple of other tricks you can form a password 'wPh1stdDl'. What are shortcomings of this and other techniques in comparison to PROPP?

Entering your password

Passwords containing capital letters, numbers and punctuation marks are mildly inconvenient to enter on the standard keyboards and extremely inconvenient to enter on mobile devices (by the way, it must be said that using non-lower-case-letter characters significantly reduces everyday usability of passwords but does not result in a commensurate increase in security against guessing

an encrypted password). PROPP passwords only include lower-case letters and are easy to enter (if you feel that using only lower-case letters may reduce security, read discussion in Section 5).

Passwords for multiple accounts

Existing suggestions for choosing good passwords state that each individual password for one account should be randomised and each of them should be memorised. However, this is not a realistic scenario for a modern user, who has 5-10 or more accounts. PROPP offers a solution which generates separate and secure passwords for each account.

Changing your password

When you or the service in which you log in using your password suspect that the password is not secure anymore, you need to find a new password. Existing suggestions for choosing good passwords do not really offer any good recommendations. With PROPP, the solution is surprisingly simple: just generate a new random part of the password for this account and keep using the old word-based part of the password. One can show that in all realistic attack scenarios this is a secure solution.

Only in extremely rare cases (for example, when an unencrypted password has been stolen) you may wish to change the word-based part of the password for each account you have. However, even then typically there will be no urgency to do this; this is what I discussed in the Acebook-Basebook unrealistic attack scenario in Section 3.

Remembering your password

If ‘wPh1stdDl’ was the only password you would ever need to remember, it would be fine – after all, this is your favourite song. However, taking into account that you have a dozen online accounts with different passwords, and some of these accounts insist on you changing your password every several months, memorising up-to-date passwords for all accounts is not realistic. If you use PROPP, you only need to remember two meaningful words and hardly ever change them.

5 PROPP in five years’ time

Will PROPP become unusable when computers work faster and can guess an encrypted PROPP password reasonably fast? No, just use this simple solution: instead of a five-letter random part of a password, use a longer random sequence of letters, for example, 8 letters. The rest remains the same as now.