Freie Universität Berlin

eAS – IT-Sicherheit

An easy way to remember passwords

In this day and age of electronic communication, who has not read guidelines or heard advice on how to choose a safe password?
In theory a password should have at least 8 digits which include upper- and lower case letters, numbers and special characters, but most importantly you are not allowed to write it down. Hence, how good is the best password in the world if you cannot remember it?

Inevitably almost every internet user is confronted with the problem of choosing a safe password. If we take into consideration that most internet users have a variety of accounts such as: email-address; chat lines; online banking; eBay account; etc. The problems concerning a safe and unique password which can be remembered for each account are increased.

On average, it is assumed that every internet user utilizes about ten passwords. To remember ten different and autonomous passwords, which all comply with the security standards is not an easy undertaking. Consequently users tend to employ easier passwords, use the same password all the time or make use of password tools.
Needless to say, all these methods involve a major lack of security.
For example, easier passwords such as the name of one’s boyfriend or girlfriend might be simple to remember, however, they hardly offer any protection. With specialized software tools this kind of passwords can easily be encrypted.
If one uses the same password all the time, intense hacking attacks could get access to an account, once an account is broken further accounts are then exposed.
Password tools are not a safe solution, they are extremely vulnerable should an attacker gain access to the users system.

However, there exists a solution to create as many passwords as one needs without remembering one completely, the algorithmic password. With this method one has to think of a stable algorithm (which means a rule to derivate a password), which nobody apart from the user knows and from which they can derive the password for every internet service. Depending on the level of difficulty and complexity of the algorithm the password is essentially secure. The following example shows precisely how one might create a password.

Algorithmic Password:

The aim is to create a password which consists of two parts. One is fixed and the other is variable. The password structure for this example is as follows: “fixed” + “variable” + “fixed” and our fixed passwords are “ZEDAT” and “O7”. These features remain constant and are only known to the user.
To obtain the variable part of our password we require an algorithm. The algorithm is to be based on the internet service where we want to use the password. For example: www.amazon.de. Here it is possible to integrate the last syllable in our password so that we get „ZEDATzon07“. If we require a password for a www.youTube.de account, the same algorithm would give „ZEDATtube07“. Using this system it is possible to add more factors to the password, for example: We can add the number of letters and vowels from our internet service. In the case of Amazon, we would obtain 6 letters plus the number of vowels, which is 3. As a total number we get 63. This number can then be added to the variable part of our

password. Resulting in „ZEDATzon6307“. Using the same scheme for You Tube, one would get 7 letters and 4 vowels („ZEDATtube7407“).
These passwords are relatively secure and extremely difficult to determine the system they are based upon. In this case, the user only has to remember the algorithm applied to obtain the password. This method allows for flexibility and easy application to create many passwords none of which have to be remembered!

Depending on the composition and complexity of the algorithm the password can be made as intricate as one wishes. For instance, it would be possible, to create a password which consist of several variable parts. (“fixed part 1” + “variable part1” + “fixed part 2” + “variable part2”). Additionally, the password could contain special characters. A method to remember the special characters might be to obtain a number which derives from the syllables and vowels. For example: “743” and replace these numbers with the special characters on the keyboard above them (“/$§”).

The crucial advantage for the use of algorithmic passwords is that with this method it is possible to create many different and relatively complex passwords which contain the adequate level of security. Furthermore, the user is no longer required to remember each individual password, only a single algorithm which they used to create their passwords.