Password Security in Practice

Sun Bingyin
Email: binsu731@student.liu.se
Supervisor: Viiveke Fåk, viiveke@isy.liu.se
TDDD17: Information Security Course
Linköping universitet,Sweden

Abstract

The widely used password technology causes it to become the target for attacks. Correspondingly, the multifarious suggestions and policies of creating a safe password emerge endlessly. As far as we know, those policies are sound enough, while the certain information/data about their actual influences still remain fuzzy. Through investigating about 275 staff in a company, the influences of suggestions and policies are surveyed and analyzed. Moreover, based on the code-breaking method, the effects of password security in practice will be expounded.

1. Introduction

As one of the authentication methods, accounts protected by password are already applied to a variety of fields, such as e-mail, online banking and some entrance guard system. Meanwhile, it also became the most insecure authentication method. The notorious issue of password stealing is not a new crime. A short and simple password will bear more risks of password attacks. Sometimes, the harm caused by password theft not only causes economic losses, but also results in psychological injuries. Consequently, in order to avoid the potential pilferage of password, setting secure passwords would be the foremost and primary measures generated in users' minds.

There is no absolute secure password; any safe or unsafe is not absolute, but relative. Comparatively speaking, a good password is hard to guess and easy to remember [1]. Meanwhile, correct password usage behaviors are also of the most importance. In order to help users create good passwords, almost every site has relative restrictions and advices on passwords setting when users register new accounts. Based on the recommendations, users can set a reliable password, combined with users' personal preferences or habits. That seems a quite good way to generate a secure password, but what is the actual situation? Will those advices influence the users' behavior? If it does, what is the extent/level? Also, this paper will focus on password usage behaviors and storage.

2. Background

There is an old saying, "A person of high position is liable to be attacked". As the most widely used method, passwords also became the most insecure authentication method. The ubiquitous passwords provide lots of opportunities to hackers who pursue their mysterious aims. In December 2009, hackers posted 32 million passwords to the internet without any further information [2].

What caused the quite high rate of password theft? The close relationships between password theft and password setting and usage behaviors are regarded here.

Further analysis on this issue will be discussed combined with the code-breaking method.

The method for code-breaking of internet passwords can be classified as follows (In this report, we just talk about the methods which relate to password practices):

1. Brute-force attack method: A trial-and-error attempt to violate the computer security by systematically attempting to use a very large number of possible passwords or keys [4]. If the combination of letters in the password is short and simple, it would be easy to suffer brute-force password attacks. At present, many code-breaking software are based on this principle.

2. Psychoanalysis: By analyzing the users' psychologies and password setting habits, the hacker can increase their working efficiency and accuracy [5]. Just think of what you can hide when you face a crafty psychologist.

3. Password usage with bad habits: Using passwords with some bad habits will also result in a password theft. For instance, writing down the password on a paper saved improperly, or sharing the password with anyone else.

We can discern that code-breaking methods are mainly aimed at password setting and usage behaviors. An oversimplified password generally means that it will be easier for a hacker to crack. Users' indiscretion will also give hackers a handle to decode the password casually. Absolute secure passwords don't exist. For instance, a good password is harder for hackers to decode, and also implies that it is harder for the owner to remember, data integrity is typically verified as a side effect of confidentiality [8]. In this case, the owner of the password may write down the password somewhere, but he or she also made a mistake at the same time. This example demonstrates that a secure password is not just a good combination of numbers, letters and characters, correct password usage also could not be neglected.

3. Survey

About 300 staff from a Chinese company participated in this survey. The average age of participants is 28. The final data analysis is based on the 263 valid questionnaires.

The password practices survey was created and accessed using Google Doc. Participants received the survey via e-mail and filled them online. Furthermore, the result we need would also be visible via Google Doc.

This section analyzes the restrictions and suggestions on password setting in depth. A survey was developed to gather the research data.

3.1 Restrictions on Passwords

"To create a password, you must follow these tips:
1. At least 6 characters.
2. A combination of at least two of the following: uppercase or lowercase letters (A-Z or a-z), numbers (0-9) and special characters (?_!@#) (example: Beatlesfan#28, &uperman1963)" [3]

Those restrictions were quoted from a famous website. Some of them even have the enforced restrictions like: Your password can't be similar to your email address or user ID [3]. Websites with such kinds of restrictions generally involve more personal

information, such as credit card information and so on.

Usually, password strength is associated with password setting. It is regarded as a measure to evaluate the level of difficulty of a password in resisting guessing and brute-force attack [6]. Password strength tries to estimate the approximate time hacker needs to find out the password so as to gain access. The strength of the password normally is described as "strong" or "weak". Some password strength can estimate the time needed to decode a password by using brute force methods [7]. For instance, a weak password, "123qwe" can be cracked easily in less than one second.

If users took those suggestions to heart and set their password with a combination of uppercase or lowercase letters, numbers and special characters, this will greatly enhance the strength of passwords apparently. The password "$uperman1963" is regarded as a strong password, and it will take 110698 years and 7 months for a hacker to crack it with brute force methods, which sounds like the story in Arabian Nights.

If rarely a password such as "$uperman1963" can be cracked handily, there must be something wrong with the password usage habits, or the hacker can read minds. if so, users can't possibly protect their passwords.

In order to help users to avoid the password usage lapses, some mature websites also give further tips on password usage suggestions. Those recommendations are often not mandatory and they only try to arouse user's awareness. Sharing a password with others servers is a typical example. Password are best kept secretly, even if you trust your friends you can never guarantee that they will be as careful as you to protect the password.

Some restrictions and suggestions are listed in Table 1. For some websites, some restrictions are enforced.

On Password Generation Practices	On Password Usage
1. Password length 2. Cannot be the same as your email address. 3. At least one alphabetic character (A-Z). 4. Don't use personal information that others can easily obtain or guess.	1. Do not share your password with others. 2. Do not use the same password for your other online accounts. 3. Keep it in mind; do not write down your password.

Table 1. Restrictions and suggestions excerpted from websites

By learning the restrictions and suggestions from various websites, it is easy to detect that all the advices usually can be split into two branches, one is password setting, and the other is the usage of password. A relative safe password needs both branches to complement with each other.

3.2 Categories of Passwords

A website provides a list of the worst passwords. It is not difficult to find that they can be divided into several categories.

In addition to passwords which only contain simple sequences of numbers, users also prefer to pick some personal meaningful information as the whole or part of their

passwords. This includes birthday, name, location, or other personal meaningful numbers and words. Those passwords have the common property: they are all easy to remember. While in the mean time, another problem emerges that other people who are close to the user may be able to guess the correct password with no difficulty.

The table below shows the categories of the passwords.

Categories of passwords
Meaningful numbers (Birthdates, phone numbers)
Names (friends, locations, pets etc.)
Simple sequences of characters(123, abc)
Meaningful words (words can be found in dictionaries)

Table 2. Categories of passwords.

3.3 Questions in the Survey

The questions in the survey were based on the study of the restrictions and suggestions on password.

The survey began with the basic background of the respondents like age; gender and internet usage behaviors. The following questions in the survey probe the password practices of the participants. Those questions are divided into three main areas as follows:

1. Password generation practices.
2. Impact of restrictions on setting a password.
3. Measures adopted to save and use passwords.

4. Results

The results of this questionnaire were reflected in the following charts.

Figure 1 revealed that most of the respondents (175, 66.53%) use a password which contains at least seven characters. Among those 175 respondents, there are 47 respondents who even use passwords where the length was more than ten characters.

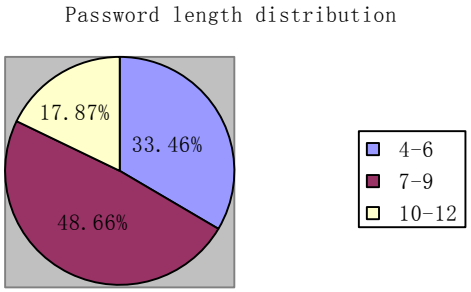

Figure 1. Password length distribution

As shown in Figure 2, less than 3% (7) of the respondents use special characters in their passwords. About fifty-five percent of the passwords only contain one element, possibly lowercase letters or numbers. The rest of the respondents (42.20%, 111) said that their passwords contain two kinds of characters.

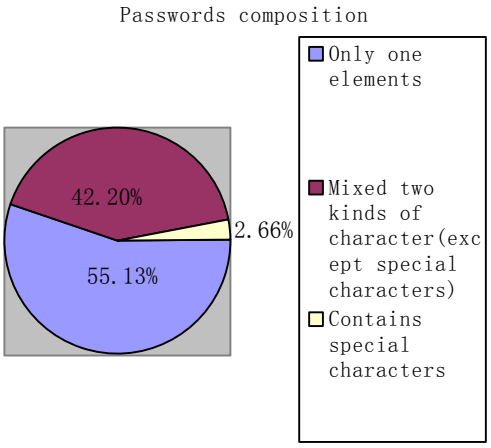

Figure 2. Passwords composition

Figure 3 illustrates the information on password generation practices. Only

approximately 11% of the respondents reported that they never use meaningful words, numbers or simple sequences of characters in their passwords. In contrast, 89.35% of the respondents (235) chose those meaningful words and numbers as their passwords.

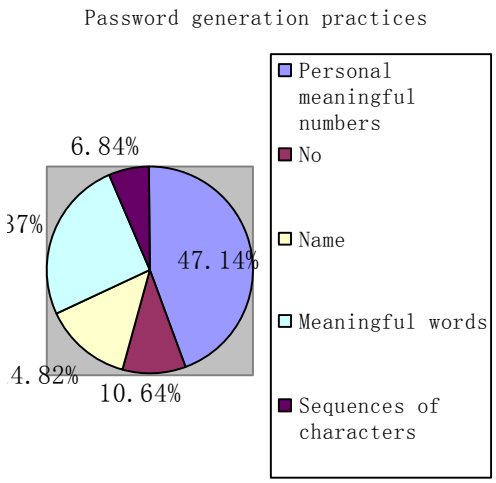

Figure 3. Password generation practices

Overall, 60.44% of respondents (159) do not use the same password for multi accounts, among those 54.08% (86) participants use variations of the same password for different accounts, for example, “abc123” for account A, and also “123abc” for the other account. The number of respondents who use exactly the same password for the different accounts is 104, close to 40%.

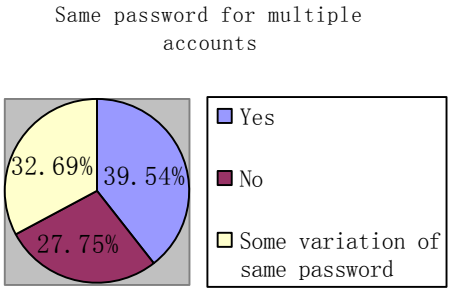

Figure 4. Same password for multiple accounts

More than half of the respondents (54.37%, 143) verified that those restrictions and suggestions really produced some effects on their passwords setting process. While 20.53% of the respondents said that they have never been affected by those restrictions and suggestions. 66 respondents reported that they take those suggestions sometimes.

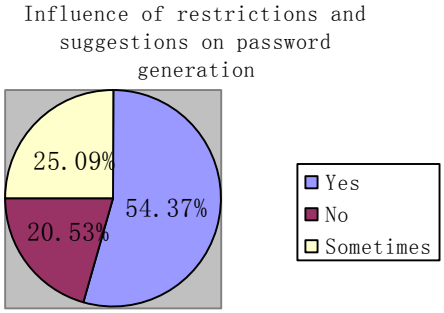

Figure 5. Influence of restrictions and suggestions on password generation

Figure 6 shows the frequency of changing password. It is apparent from the chart that most of the respondents never change their passwords. The number of respondents who change their passwords periodically is only 47. 20.53% (54) respondents changed their passwords for a particular reason.

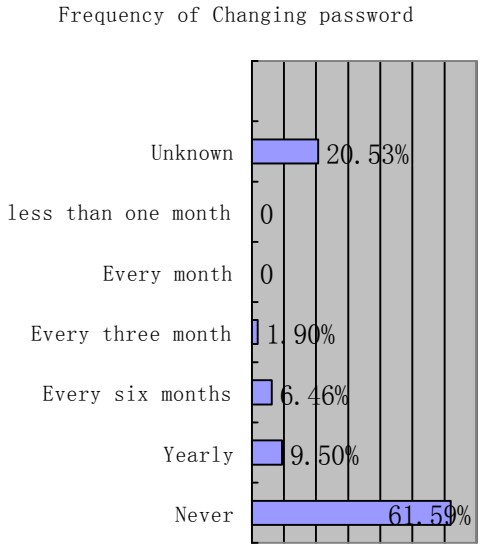

Figure 6. Frequency of changing password

When asked “How do you store your passwords?” 65.39% respondents said they

keep the password in their mind. This is a safe way to save the password. However, how many of them use different passwords for multiple accounts? This is a question worthy of consideration. And the other 34.60% people said that they are in the habit of writing down the passwords.

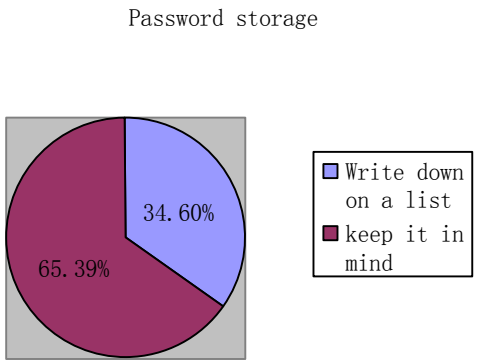

Figure 7. Password storage

Obviously, over half of the respondents (67.68%, 178) shared their passwords with others, while 32.31% responded that they do not give their passwords to anyone, even their parents.

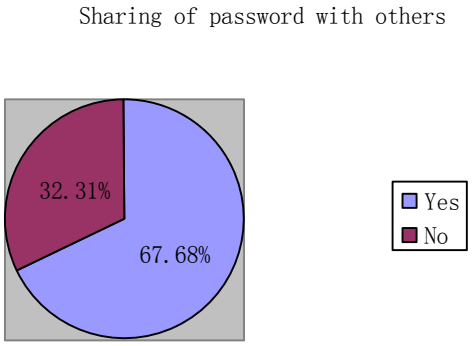

Figure 8. Sharing of password with others

5. Discussion

It is conceivable that once the password is lost, how heavy the losses depend on the person or enterprise! Unfortunately, the figures lead us to the conclusion that most respondents in this study did not attach great importance to the restrictions and suggestions of setting a secure password. Consequently, they have insecure passwords and perhaps, some of the respondents were already attacked by the hackers without detecting the fact.

In this survey, approximately 90% of the respondents chose meaningful words, numbers or simple sequences of characters as their passwords. However, hackers reply to these kinds of passwords scornfully.

First of all, simple sequences of characters were examined. It is said people prefer to use “123456” or “654321” as password [2]. By using brute-force attack tools, the hacker is able to get access to the personal accounts if the passwords are like these, and they even don't need to use the permutation and combination methods.

While for those who use personal meaningful numbers as passwords, there still exists a cracking method. For example, “19860705” is an 8-digit password. There are 10 numbers to choose from (0, 1….9) for each digit position, so there are 100000000 permutations. It is a terrible workload for humans, but not for computers. It just needs several minutes to test all the permutations by using a powerful computer. In addition, no matter what the format of the number is (yyyy-mm-dd or dd-mm-yyyy); this kind of passwords can be decoded quite easily. The same principle is valid for the telephone number, even though a telephone number has

more than 11 digits. Users have to realize that the complexity of a password is not just based on the length. A 15-digit number password is not necessarily more secure than a password mixed with letters, numbers and special characters.

And that is also applicable for passwords which only contain letters and just need more time to test the permutations.

Users choose meaningful words, or numbers as their passwords, and it enables the users to remember their passwords easily. While this also means that the hacker who is close to you can decode your passwords easily.

Getting rid of bad habits of password usage is also very important. The results of the investigation indicated that correct password usage was not paid enough attention. Sometimes people share passwords because they need to help others or need other people's helps. They should try to find other ways rather than share passwords. If password sharing still cannot be avoided, they should change their passwords immediately after sharing passwords with others. Sharing passwords is also considered as a sign of intimacy, while safety should always be the primary issue in any case. Changing password infrequently and incorrect password storage also brought potential risks to password security. Even though most users cannot endure changing passwords frequently, periodic changing is still recommended to reduce the probability of suffering an attack by brute force since passwords can be guessed over time. Another common password security issue is that some people write down their password and place it somewhere. Frequently changed passwords and complex passwords are two main reasons that lead to users writing down their passwords and leaving them in insecure locations. If you must write down your passwords, at least keep it somewhere that is difficult for others to find.

6. Summary

Although stealing passwords has taken place repeatedly around us, it still cannot arouse our adequate awareness. A good password should contain at least four different types of characters and eight characters, and it should not be a meaningful word or number. In addition, the norms of the usage of password must be standardized.

7. References

[1].Password Memorability and Security: Empirical Results
http://homepages.cs.ncl.ac.uk/jeff.yan/jyan_ieee_pwd.pdf March.2010.
[2].WP_Consumer_Password_Worst_Practices.pdf
http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf
March.2010.
[3].Restrictions on creating a password
http://pages.ebay.com/help/new/contextual/create_password.html April.2010
[4].Exhaustive Attack
http://www.its.bldrdoc.gov/projects/devglossary/_exhaustive_attack.html March.2010.
[5].Password attack methods
http://www.williamlong.info/archives/1264.html March.2010
[6].Password definition
http://en.wikipedia.org/wiki/Password
March.2010.
[7]Password Strength
http://www.unwrongest.com/projects/password-strength/ April.2010
[8].Dieter Gollmann: Computer Security, second edition