Password in practice

- An analysis of efficiency of password management against attack among students

Eric Gustafsson Jizhi Li
Email: {erigu155, liji050}@student.liu.se
Supervisor: Jan-Åke Larsson, {jan-ake.larsson@liu.se}
Project Report for Information Security Course
Linköping University, Sweden

Abstract

The purpose of this paper is to analyze how people with computer experience handle their passwords, in order to see what type of information that should be used to increase the user security. Since the users are the weakest link when it comes to computer security and since their interests in security is usually low, it is important that users are encouraged to improve their security in an efficient way. With the intention of studying the behaviors of the selected group, we send the surveys to students at Linköping University. They either study computer science or have computer science as a technical profile, so we can make sure that they use passwords frequently.

From the empirical study of the survey results, we have discovered that most of the survey participants are trying to choose a good password and most of them are trying to improve their password management by i.e. increasing the complexity of passwords. However their password management is doubtful. For instance, 62% users reuse their passwords on important websites and 28% users never changed their passwords. Therefore we consider that it is more than necessary to give them a worthwhile password management solution. With both security and user-friendly perspectives, we discussed if using a password manager application is the best solution to improve their password management.

1. Introduction

Password management is part of our daily life; almost everyone uses some sort of passwords. There are very few people who do not have to remember at least one password in today's IT-intensive worlds. Every day we use passwords to access bank accounts, our computers, and various social websites. Passwords are the most common way to authenticate to applications and the number of applications that requires passwords continues to increase[1]. Thus people are facing a situation where they may be required to create and handle more than a dozen passwords.

In order to create a safe password it must be complex enough to make other people unable to guess it while it is easy enough to remember.[2] Users can also follow password security guidelines to make sure that their passwords management is safe, but these guidelines can sometimes have a reversed effect on security[3]. So, how should users use those guidelines in password management?

The weakest link when it comes to security is often considered to be the users. The attacks for passwords are more and more directed towards the users. The users must be aware of what potential risks they may face when there are attacks on their passwords.

This paper intends to find out the answers to those questions and problems by studying how students handle their passwords and understand how likely they are to be victims of an attack. In the end of the paper we will also discuss if there is any silver bullet to reduce the likelihood of a successful password attack.

1.1 Purpose

The purpose of this paper is to give some hints to students, for them to improve their passwords, through analyzing if their password management is efficient against various password attacks.

This will be done by:

- Studying user behavior of password management through surveys.
- Studying different kinds of password attacks.

[1] (Beate Grawemeyer and Hilary Johnson, 2011)

[2] (Bradley, 2006)

[3] (Anne Adams and Martina Angela Sasse, 1999)

- Analyzing the potential risks in their password management, based on the survey result.

2. Background

A reason why the importance of password strength should never be underestimated is the fact that password authentication is not only important to service user, it is also important to the service providers. Once passwords are lost, it will cause a lack of trust for the service provider. A hacker group managed to steal user passwords from Sony the year 2011[4]. Which led to a lawsuit against Sony who also went out with a formal apology.

A survey in *Essential computer security*[5] discovered that 58 % of employees at an IT-helpdesk had more than six passwords to manage, and half of those have more than 13 passwords to manage. Adams and Sasse[6] recommend users to have no more than five passwords to memorize. When this limit is exceeded the memorability goes down. This is an impossible equation if the passwords are to be unique. Users are usually not very concerned with security and the increase of applications requiring password authentication has led to the same passwords being reused or reused with minor changes.

The users' initial lack of interest for security may lead to the user choosing a weak password[7]. It is possible to give the user a machine generated password but it will be harder for the user to remember[8]. To increase the security, it is possible for hosts to put restrictions and requirements on passwords to force the users to pick a stronger password. Some restrictions do however have an opposite effect since they are seen as an annoyance by the user.

3. Theory

3.1 Common password weaknesses and attacks

In this chapter, different attacks on passwords will be presented so there will be something to check against. Then guidelines for safe passwords will be presented to see how different theories believe passwords ought to be managed. Afterwards the statistical methods that are used in the report will be presented in order to see how relevant the surveys might be.

The method of cracking passwords varies on different kinds of the target system. For instance, online system attack may be harder due to some password authentication systems have protocols that will lock the account for a while after several failed attempts.

The automated password attempts per second are also limited by the Internet speed and server authentication response speed on an online system. However, there is no such protection for offline attacks. Offline attacks are only limited by the attack method and attacker's CPU power and patience[9].

3.1.1 Guessing attacks

Guessing attacks are very common and sometimes a very efficient way to crack a user's password on user side. With the development of both hardware and software algorithms, guessing attacks against the passwords with shorter length and less complexities are very efficient. According to a very famous password cracker tool Hashcat[10], they claim that they can achieve more than 140 billion password attempts per second with a normal 8 core AMD R9 29X CPU on stock core clock. This makes all kinds of guessing attack methods much more efficient and force us to increase the complexity standards of a safe password.

Why is that? Let's say that we are using a password that considered being good enough with 8 characters, mixed with only numbers and upper/lower case letters. (62 characters in total) The total combination for the password will be $62^8 \cong 2.2 \cdot 10^{14}$, which is around 220,000 billion. It means that even with the worst case, it will only take about 26 minutes to crack the password by using brute force.

Although the speed of password attempts are usually limited by the speed of internet and password authentication protocol on server side, it still gives us a general impression of how fast nowadays computer can crack password on an offline local machine and threaten the password management.

Brute force attacks[11]

[4] (BBC, 2011)

[5] (Bradley, 2006)

[6] (Anne Adams and Martina Angela Sasse, 1999)

[7] (Beate Grawemeyer and Hilary Johnson, 2011)

[8] (Cheswick, 2013)

[9] (Burnett, 2006)

[10] (Hashcat, 2014)

[11] (Bradley, 2006)

Brute force attacks are usually a common name of all kinds of guessing attacks. Pure brute force attacks will try all different combinations. This method can break all types of passwords if provided enough time or process capacity. The only efficient and also the best way to protect your password against such kind of attack is to have a password with high complexity and sufficient length. If we are using a password combination with all common symbols, upper and lower case alphabet plus numbers (96 characters in total) and password length at 10. It will takes more than 15 years for Hashcat to crack it.

Dictionary attack[12]

Dictionary attack is another type of guessing attack. Threat agents will try to guess user's password by using common dictionary words (in many languages). The attackers usually use a word-list and try all the combinations of words up to a certain length. Nowadays, there are many word lists on Internet that are specifically designed for dictionary attacks. Attackers can easily find them on many websites such as wordlist.sourceforge.net. The word list doesn't only contain word, names, inflections, phrases, abbreviations and hyphenations in English and also other common languages.

Hybrid attack[13]

For those passwords that are combined by dictionary words and some extra random characters, attacker can crack the password by using a so called hybrid attack. It will crack the password by combining possible dictionary word or names with some extra random characters.

Smart guessing[14]

Smart guessing is a method to gain user's password by simply try the most common passwords on a large number of accounts. Just like the word list, there are many common password lists on the website which contain the most used passwords. Mark Burnett[15] made a list of 10,000 most common passwords and by comparing this password list with about 6,000,000 unique username/password combos he collected. He found out that:

- 4.7% of users have the password *password*;
- 8.5% have the passwords password or *123456*;
- 9.8% have the passwords *password*, *123456* or *12345678*;
- 14% have a password from the top 10 passwords;
- 40% have a password from the top 100 passwords;
- 79% have a password from the top 500 passwords;
- 91% have a password from the top 1000 passwords;

It means that with his top 10,000 password list, attacker can easily crack more than 91% of user's account immediately and even an online system with proper authentication protocol protection, it also shows that smart guessing with password list is a feasible attack method.

Another way of smart guessing is to use a cracked/leaked password from a user's account and try this password on all the other accounts that belongs to this user.

3.1.2 Other attack techniques

Rainbow tables

By hashing billions of normal words an attacker can create a table to which he or she can compare password hashes that are stolen. Once a match to hashes is made, the attacker knows the algorithm used to hash the password and can from there deduct the original passwords from the hashes. The tables take a long time to generate and it takes a long time to match the hashed passwords to the tables.

By at first hashing for example the word password in different ways, then compares them with the stolen hash values; the attacker will probably get a match since it is a common password[16].

Social engineering

Social engineering attacks can be divided into human based and computer based. In human based attack, attacker can for instance pretend to be an employee or any valid user on the system and ask the administrator for the password.

The most famous computer based social engineering attack is called phishing, phishing attacks involves fake email, online chat or using hijacked websites etc.

Social engineering attacks are mostly efficient against those users or administrators who are careless.

Key logger

Unlike the other attack method, keyloggers intercept the user name and password by intercept the data of key-strokes. This attack method doesn't need a lot time to crack the password, once the user enter the password, the attack will obtain the user name and password immediately. It usually considered as the easiest way to obtain passwords from user.

Even though there are many anti-keylogger softwares on market today, none of them can promise the user that they can detect all kinds of keyloggers. This leaves us a big potential of having a keylogger installed and we yet have no knowledge about it.

[12] (Bradley, 2006)

[13] (Bradley, 2006)

[14] (Bradley, 2006)

[15] (Burnett, 2011)

[16] (Burnett, 2006)

How can we avoid password being exploited by keyloggers? Frank Nielsen from Cornell University once suggested using color pins to avoid keyloggers[17].

His system doesn't require any mouse or key clicking, which gives key logger nothing to record during the login. Another way is to use password management software. User may save the passwords in the manager at a safe environment and then use the password by directly withdraw the password from manager.

3.2 Password management guidelines

The very first, famous and widely used recommendation for choosing a password is from the Password Management Guideline published by Department of Defense in 1985, as known as the Green book[18]. The guideline prescribed five essential aspects and three major features of a password system.

The ones that related to user's behaviors are:

1) A password must be initially assigned to a user
2) A user's password must be changed periodically;
3) Users must remember their passwords;
4) User should be able to change their own passwords;
5) Passwords should be machine-generated rather than user-created.

However, the guideline is almost 30 years old and some of the rules do not apply to today's security situation.

William Cheswick did a comprehensive discussion of how the rules shall be updated and optimized in his article "Rethinking passwords"[19]. He writes that rule 1, 4 and 5 are still fine nowadays, but the others should be improved. For instance, rule 3 is unreasonable, especially for machine-generated password. He also believed that changing password periodically is a good idea, but it doesn't have to be a strict requirement.

Bruce Schneier, an American famous cryptographer, computer security and privacy specialist, published an article[20] in the year 2014 on how to choose secure passwords. Besides his password selection scheme, he also mentioned four recommendations:

1) Never reuse a password you care about.

2) Don't bother updating your password regularly.

3) Beware the "secret question", better to use a password manager or to write your passwords down on a piece of paper and secure that piece of paper.

4) Seriously consider using websites that offers two-factor authentication.

3.2.1 Password selection guideline

There are many different recommendations of how to select a good password nowadays. Garfinkel and Spafford introduced one of them in 1996[21]. According to their guideline, a secure passwords should not include: e.g. anybody's name; your phone number; a place; a proper noun; a word in any dictionary; passwords of all the same letter; simple patterns on the keyboard; any of the about spelled backwards; any of above followed by a single digit.

A secure passwords shall contain both upper and lower case letters; have digits and/or punctuation characters as well as letters; are easy to remember, so they do not have to be written down; are seven or eight characters long; can be typed quickly, so someone else cannot look over your shoulder.

Another often-cited password selection scheme is from a XKCD comic[22]. They have some different views on how to choose a hard-to-guess password than Garfinkel and Spafford. In their opinion, a password combined by several random common dictionary words can also be a good password. However, this conclusion is disagreed by Steve Gibson, American software engineer and security researcher on his podcast "Security Now![23]"

3.2.2 Password storage management guideline

Today, more and more users are facing a same problem, handling multiple passwords. From a security aspect, users shall not reuse any password and the passwords shall be hard to remember or at least complicated, which simply made it almost impossible for users to remember all the passwords without writing them down or use a password manager.

Writing down the password on paper was the most recommended solution for managing multiple passwords, until password manager came out. There are mainly two types of password managers, portable and online manager. Due to a survey study[24] published on 2010 international information security and cryptology conference, there are significant more users prefer to use

[17] (Nielsen, 2013)
[18] (Department of Defense , 1985)
[19] (Cheswick, 2013)
[20] (Schneier, 2014)
[21] (Simson Garfunkel and Gene Spafford, 1996)
[22] (Munroa, u.d.)
[23] (Wiberg, 2011)
[24] (A. Karole, N. Saxena and N. Chrisin, 2010)

a portable password manager than online manager due to both security and usability reasons.

Nonetheless, the security issue of password manager is still questionable. Due to a study[25], modern browser online password managers are very vulnerable against specific attacks.

3.2.3 Using graphical password as alternative

In the beginning of 1999, graphical password was introduced as an alternative password scheme, motivated by the promise of improving password memorability and usability.

Memorability

Dual-coding theory[26] is the most famous theory suggesting that verbal (word-based) and non-verbal (image-based) memory are represented differently in brain. Image-based memory can be memorized directly by brain, which makes it much easier for human to remember. Word-based memory, on the other hand, requires additional processing to memorize.

Usability

Nowadays there are mainly three types of graphical password system, recall-based system, recognition-based system and cued-recall system. Recall-based system requires user to draw a certain figure or fill certain tiles with different colors. Recognition-based system will provide user with certain information, pictures or patterns for instance and then let them decide if it matches certain information previously memorized. According to many existing theories[27], Recall-based memory is much more complicated and harder for user to adapt.

Cued-recall system, require user to remember and target specific location within an image. According to the study[28], it reduced the memory load on users and it is easier than normal memory recall.

Security

There is always a concern about the security level of graphical password, as a graphical password doesn't have as many variations as text password. Oorschot and Thrope's study[29] on exploiting a cued-recall graphical password system shows that within 3 guesses, there is a 7-10% chance for the threat agent to exploit it. With such a high vulnerability rate, it is really hard for service providers to use it for a high security level authentication process.

4. Empirical study

4.1 Empirical method

Our research aim is to investigate how people with computer science knowledge background manage their password. Most of our research participators are from university with specialized field in computer science. Specifically, we want to find out how people manage their password in following areas:

- How do people select their passwords?
- Is the Green Book's recommendation followed by most users?
- How do people manage multiple passwords with different websites?

The reason for choosing students with computer science specialization is because we believe that they are managing their passwords in a more proper way and need to manage more passwords than other people. In this situation, we can also assume that they are representing normal people with best behaviors in password management.

University students were invited to complete a web-based survey about their password management behaviors. We've chosen about around 300 students with computer science educated background as the survey pool, however even they were told that the survey is only for a research purpose and we are not going to abuse their answers or link the questions with their names or email accounts, only very a few students were willing to participate in our survey. Which on the other hand can be seen as a very cautious action to protect their personal information.

For the participators who were willing to join the survey, they were asked with 8 questions and those questions will reflect their password management behaviors in following area.

1. Password change frequency.
2. Password selection scheme.
3. Do people reuse their passwords?
4. Will the password recommendation on website help people to choose a better password?
5. Do people use password manager?
6. Do people avoid using real answer to password recovering question in case to increase the secure?

The first password management behavior is very neutral and is neither good nor bad, we only want to see

[25] (R. Gonzalez, E. Y. Chen and C. Jackson, 2013)

[26] (Paivio, 2011)

[27] (R.Biddle, S. Chiasson and P.C. van Oorschot, 2012)

[28] Ibid

[29] (P.C. van Oorschot and J. Thorpe, 2011)

if changing password periodically is a common behavior and if it is acceptable and widely used by common folk.

The second behavior shows us the password selections that are used by users. From the answers to this area we may see if most of the users are doing fine or if their password selections makes their passwords very vulnerable against certain attacks.

The third and sixth behaviors are the ones that we want users to avoid. And the rest of behaviors can help us to find a way to help them to improve their password management with an acceptable and feasible way.

4.2 Survey result

A total of 21 participants from university completed the survey. They were also allowed to not answer all the questions. We've arranged the questions in a way so that all the participants will not release any personal sensitive information from the survey.

1) Do you change the password:
   a. Never change password (not due to a system mandatory request). **6(28.6%)**
   b. Change password regularly. **3(14.3%)**
   c. Only change password when you suspect that the password is compromised. **11(52.4%)**
2) Do you use password with mixed upper/lower cases alphabets, common symbols and numbers?
   a. Yes. **17(80.9%)**
   b. No. **2(9.5%)**
3) Does your password contains:
   a. Any dates that have a significance to you. **5(23.8%)**
   b. Dictionary words. **9(42.9%)**
4) How many different password do you have?
   a. Less than 3. **4(19.0%)**
   b. 3 to 5. **6(28.6%)**
   c. 5 to 10. **3(14.3%)**
   d. More than 10. **6(28.6%)**
5) Do you reuse any password that you care about?
   a. Yes. **13(61.9%)**
   b. No. **8(38.1%)**
6) How will the password requirement/recommendation on the website affect your choice of password? (E.g. password strength indicator, recommended password pattern.)
   a. Doesn't affect me at all. **11(52.4%)**
   b. I will choose a password according to its suggestion. **10(47.6%)**
7) Do you use any password management software to handle your password?
   a. Yes. **4(19.0%)**
   b. No. **17(81.0%)**
   c. Remember them. **5(29.4%)**
   d. Write down on paper. **4(23.5%)**
   e. Save on computer. **2(11.8%)**
8) Do you use the real answer for the password recovery questions?
   a. Yes. **7(33.3%)**
   b. No. **13(61.9%)**

5. Analysis

We analyze the behavior of all the participants by using the answers from the survey and password attack methods.

Password change frequency

When people were asked about if they are used to change password periodically, only 14.3% of users answered yes and about half of those who answered no don't even change the password even they suspect that the password is compromised. This may just give attacker a big opportunity and even longer time to crack the user's other accounts and lead to a much bigger damage impact. For instance, attacker can use smart guessing method to test user's exploited password and s/his email on all the other social networking account.

Even though the password guideline from the Green Book suggested user to change password periodically, many security specialists i.e. Bruce Schneier and William Cheswick briefly discussed and indicated that it is not really necessarily to update password regularly. Therefore we won't neither make any justify on participants' behavior on it.

Password selection scheme

Participants were asked 2 questions about their password selection. On the one of "if they are using password mixed with upper/lower case alphabets, common symbols and numbers", more than 80% of users gave positive answers. From the theory part of attack methods, we know that a complicated password with well mixed character will take a very long time for attacker to crack by using certain guessing attack methods, such as brute-force.

However, about 70% of users' passwords contain dictionary words or special dates. (E.g. birthday) Which makes their passwords still very vulnerable against smart guessing or hybrid attack.

Do people reuse their passwords?

It is not a surprise that 61.9% of users reuse their password. Reuse password may make it much easier to manage multiple passwords, but it has a high security risk potential. Once an account is compromised, further attacks on this user's other accounts will also be successful. The attack method smart guess is especially for this behavior, therefore it shall be strictly forbidden in any good password management.

Will the password recommendation on website help people to choose a better password?

The result is approximately half and half. 52.4% of the user said that their password selection is not affected by any password strength indicator. And rest said that they will follow it until the strength indicator agrees that their passwords are strong enough.

In our opinion, the password indicator may not perfectly represent the strength of a password against all kinds of attacks, but it does show the complexity of a password. (E.g. on www.passwordmeter.com, password *!"#123qweQWE* has a 100% score, but it is one of the common password that has been used and quite vulnerable if the attacker uses smart guessing with a password list.)

We can't rely on the score of a password indicator; it only provides users with a good indication about the complexity of the password. The user shall use this password strength indicator and other method to select a better password.

Do people use password manager?

Only very a few users (19%) are using password manager, others usually memorize the passwords by memory or write the passwords on paper. Except those who have incredible memory, it is hard for people to memorize more than a dozen passwords with high complexity, because a good password, according to the Green Book's guideline, shall be impossible to memorize.

We neither agree that use paper to record the password is a good choice. Because we concerned that once the paper is lost or stolen in purpose, all those accounts will be compromised immediately. In this paper, we consider password manager the best choice. We will discuss the reason about it in the discussion part.

Do people avoid using real answer to password recovering question in case to increase the secure?

33.3% of the users are using real answers for the password recovery questions. It makes the password vulnerable against the attackers who know the target in real life or the attackers that have any personal information about the target. Nowadays, many people publish their personal information, e.g. pet's name, born city, first high school name on social network like Facebook or Twitter. It makes it much easier for attacker to gather enough information for a password recovery. Therefore, it is definitely not a good idea to use real answers.

A strong password is good but it is not a guarantee that your account will not be hacked. A strong password protects, at least for a long time, against brute force attacks but it cannot protect against key loggers and rainbow tables. The user has to know how passwords are protected on websites

6. Conclusion

By reviewing the survey and analyses the result with password attacks perspectives, we saw that when it comes to password selection, most of the participants are doing pretty well by trying to select password carefully and improve their password selection by either using a password strength indicator or simply increase the complexity of the password. However there is still a certain risk potential within their password selection, for instance more than 70% of the participants' passwords contains dictionary words or other information that could relate to the user,

What most of the participants are not doing well is password management. The way that they manage their passwords may give the attackers many opportunities of cracking the password. The users should avoid the behaviors like reuse password, use fake answers for password recovery questions and by improving how do they save the password can also help them to handle more complicated passwords.

7. Discussion

Our suggestion for users to improve their password management with the easiest and most efficient method is to use a trustful password manager. We will discuss the reasons that lead us to this conclusion.

In order to improve users, especially students' password management, we need to discuss about those topics from both security and user-friendly point-of-view:

Will a periodically changed password more secure than others?

Not really. Both William Cheswick and Bruce Schneier stated that it is not really necessary to change password regularly. Our opinion is that user should only feel necessary to change the password when they suspect that their passwords are compromised. The reason that the Green Book suggested users to change password regularly is because they need to protect their passwords against massive potential attacks, the passwords might already be compromised without being noticed by the users. However, normal users are not under such circumstance.

Is there a way to select a password that can be easily memorized and be random enough for it being hard to guess or cracked easily with brutal force?

The Green Book says that a password that has both randomness and complexity should not be possible to memorize it. We can use certain pattern to make the complexity of a password high enough, but then it won't be random in that case.

Is reuse of password or password-pattern with few extra characters dangerous?

Yes, reuse passwords is extremely dangerous. If one of user's accounts is compromised, all the accounts with same or similar passwords will be compromised easily.

Is graphical password a feasible alternative of traditional password?

Not yet for a high secure authentication system. They could be used together with text-based password to improve the security.

Is password manager with random password generator a universal solution aka silver bullet?

It is almost certainly true. With password manager, user can save all random and complex passwords easily, change them whenever they want without forgetting the passwords. Password manager allow users to manager as many passwords as they want.

The only downside is the concern of the security of password manager itself, especially online password managers. Maybe it is not yet convincing to say that any password manager is a silver bullet, but the risk is definitely acceptable by normal users.

Final words

In order to increase security users have to make sure that their passwords are handled correctly. Since a strong password has no defense against some types of attacks. The user has to avoid websites that cannot guarantee security. It is also possible that the user, with the knowledge that the password might be compromised, stores no vital information on the site and does not use the same password on any important websites or applications. Password management software is not yet a silver bullet, but it can provide most users with a better password management. Therefore users shall seriously consider using a trustful password manager to simplify the password management.

8. References

A. Karole, N. Saxena and N. Chrisin, 2010. A Comparative Usability Evaluation of Traditional Password Managers. *Information security and cryptology - ICISC 2010,* p. 233.

Anne Adams and Martina Angela Sasse, 1999. Users are not the enemy. *Communications of the ACM,* 42(12).

BBC, 2011. *BBC.* [Online] Available at: http://www.bbc.co.uk/news/technology-13192359 [Accessed April 2014].

Beate Grawemeyer and Hilary Johnson, 2011. Using and managing multiple passwords: A week to a view. *Interacting with Computer,* Volume 23, p. 256.

Bradley, T., 2006. *Essential Computer Security.* Canada: Andrew Williams.

Burnett, M., 2006. *Perfect passwords.* Rockland: Syngress.

Burnett, M., 2011. *10,000 Top Passwords.* [Online] Available at: https://xato.net/passwords/more-top-worst-passwords/#.U1_B3fmSx8H [Accessed April 2014].

Cheswick, W., 2013. Rethinking Passwords. *ACMQueue,* Volume 56.

Department of Defense , 1985. *Password management guideline,* s.l.: Computer Security Center.

Hashcat, 2014. *Hashcat.* [Online] Available at: https://hashcat.net/oclhashcat/[Accessed April 2014].

Munroa, R., n.d. *Password Strength.* [Online] Available at: http://xkcd.com/936/[Accessed April 2014].

Nielsen, F., 2013. Logging safely in public spaces using color PINs. *Sony Computer Science Laboratories, Inc.*.

P.C. van Oorschot and J. Thorpe, 2011. Exploiting predictability in click-based graphical passwords. *Journal of Computer Security ,* Volume 19, p. 669.

Paivio, A., 2011. Dual Coding Theory, Word Abstractness, and Emotion: A Critical Review of Kousta. *Journal of Experimental Psychology: General,* Volume 142, p. 202.

R. Gonzalez, E. Y. Chen and C. Jackson, 2013. Automated Password Extraction Attack on Modern Password Managers.

R.Biddle, S. Chiasson and P.C. van Oorschot, 2012. Graphical Passwords: Learning from the First Twelve Years. *Carleton University.*

Schneier, B., 2014. *Choosing Secure Passwords.* [Online] Available at:https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html[Accessed April 2014].

Simson Garfunkel and Gene Spafford, 1996. *Practical UNIX and Internet security.* Bonn: O'Reilly.

Wahlin, K., 2011. *Tillämpad statistik.* Stockholm: Bonnier Utbildning.

Wiberg, K., 2011. *How much entropy in that password?*. [Online] Available at: https://subrabbit.wordpress.com/2011/08/26/how-much-entropy-in-that-password
[Accessed April 2014].