A Comparison of Password Management Policies

Boštjan Brumen[1], Renato Ivančič[2], Ivan Rozman[1]
[1]Faculty of Electronics and Computer Science, University of Maribor, Maribor, Slovenia
[2]ITPM e.U., Vienna, Austria

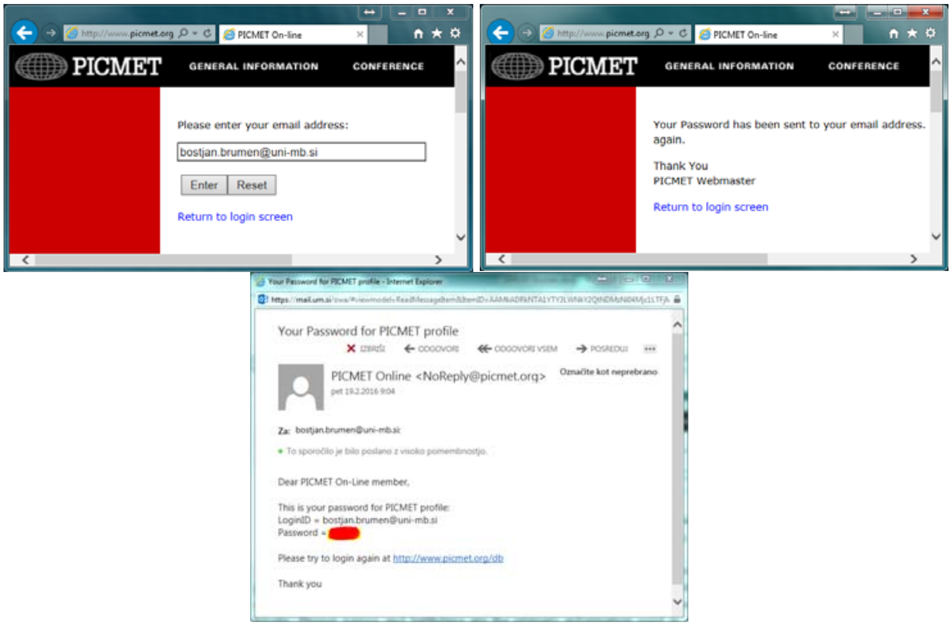
***Abstract*--Managing of passwords in information systems is a very important task, yet nothing seems to be learned from the recent stories. The consequences of bad password management practices have led to the loss of lives, as in the case of suicides after the "Ashley Madison leak". Password security is simply not taken seriously, despite problems being known since 1979 at least. Interestingly, the PICMET conference on-line system itself implements a bad password management policy as all passwords are stored and re-sent upon request by plaintext email. The objective of this paper is to present the underlying mechanisms that lead to bad password management policies. Memorability and memory decay, complexity, simplicity and other factors are presented and analyzed. A novel password management policy "Psychopass" is proposed, where a password can be created, memorized and recalled by thinking of an action sequence (visual representation) instead of a string of characters. In the experiment it was shown that users tend to better remember passwords under the "Psychopass" policy compared to other password management policies nowadays in effect. The results confirm that "Psychopass" policy is an alternative to the existing password management practices and can improve the resilience to the attacks on information systems.**

I. INTRODUCTION

Weak passwords have led to very serious breaches, exposing millions of users and/or causing billions in damages. The history of password-related problem pre-dates the seminal paper written by Morris and Thompson in in 1979 [1] – it goes way back to mid-1960s and to the CTSS operating system exposing all the system passwords as a daily welcome message [2].

Bad passwords and/or practices continue through today. To substantiate this claim let us take a look at the computerized peer review system of this very conference, the PICMET. To upload a manuscript, a user must first create an account by selecting a username and a password. If the password is forgotten, the system is able to re-send it back to the user (see Fig. 1). This is done in a plain-text e-mail, meaning the plaintext password itself is stored in the PICMET's system, and once sent by e-mail also in all the passing systems, in the end-user's e-mail box and probably also on the user's hard drive. Such a password management system is very vulnerable to attacks, either by attacking the PICMET's password storage system or by attacking any of the weak points en route. Instead of storing plaintext passwords, the system should have stored the salted hash values of passwords in combination with on-line password reset functionality. A breach of the current system could have exposed all users' account names (usually emails) and the corresponding passwords.

Breaches can have very severe consequences, such as millions in damages [3], or even losses of lives, as was the case of the Ashley Madison leak in August 2015, where several suicides are related to the leaks [4]. A comprehensive list of breaches since 2005 can be found at [5].



Please enter your email address:

bostjan.brumen@uni-mb.si

Your Password has been sent to your email address. again.

Thank You
PICMET Webmaster

Your Password for PICMET profile - Internet Explorer

Your Password for PICMET profile

PICMET Online <NoReply@picmet.org>
pet 19.2.2016 9:04

Za: bostjan.brumen@uni-mb.si

To sporočilo je bilo poslano z visoko pomembnostjo.

Dear PICMET On-Line member,

This is your password for PICMET profile:
LoginID = bostjan.brumen@uni-mb.si
Password = [redacted]

Please try to login again at http://www.picmet.org/db

Thank you

Fig 1. The PICMET system's management of lost passwords

A typical survey [6] evaluating the generation and use of passwords revealed that users have several password uses and the average password has more than one application. Two thirds of passwords are designed around one's personal characteristics, with most of the remainder relating to relatives, friends or lovers. Proper names and birthdays are the primary information used in constructing passwords, accounting for about half of all password constructions. Almost all respondents reuse passwords, and about two thirds of password uses are duplications. Passwords have been forgotten by a third of respondents, and over half keep a written record of them [6].

It seems that nothing has been learnt and changed in the course of almost 35 years – users and their passwords remain the weakest link [7-11]. The basic and the most relied-upon security mechanism in information systems is the ability to authenticate the identity of a user, although well-known systems are proven to be defective [12]. The passwords used to be [13-15] and still are the main methods of authentication [16-18], although research continues on more sophisticated methods of authentication, see e.g. [18-22].

A. Why are good passwords so hard to remember and why does it matter?

A password is considered good and strong if a brute force, a dictionary and guessing attacks cannot reveal it. A detailed discussion on password strengths can be found in [23] and [24].

The main problems with password management are:

- the users tend to choose weak passwords which are easy to guess [25]
- the users tend to re-use one password for several different purposes (accounts / web services) [6]
- the users forget passwords and, to prevent forgetting, write them down in insecure places [26-28].

The problem with bad and/or weak passwords is that an adversary can exploit a security weakness within a number of systems where such a password is used or stored. For example, if a user is using a bad password for accessing privacy sensitive data and the same password is used for insecure web log-in, an attacker can obtain access to private data by breaking into an insecure web site.

Additionally, insecure web sites can sometimes reveal data that enable an adversary to launch an off-line attack instead of an off-line attack. For example, if a system locks out the user after several unsuccessful attempts (typically: 3), an adversary has almost no chance to succeed. But, if the system reveals encrypted passwords, an adversary can launch a massive off-line brute force attack on such passwords to reveal them. Once revealed, the first attempt on the original target is successful.

Thus a security administrator must address all of the above issues in a password management policy. The first issue can be addressed by enforcing a strict password management policy that prevents users from selecting weak and bad passwords. The last two issues must be addressed by educating users.

In order to render brute force attacks infeasible, passwords should be made up of 11 or more (randomly drawn) characters [17].

But, 11 characters to remember requires more capacity than is the capacity of a human memory, where the well-known 7±2 principle applies [29]. Human memory in addition is temporally limited (short-term) when it comes to memorizing sequences [30]. For this reason good passwords that are consisting of an abundant number of randomly selected characters are doomed: the users will either forget them [25] or write them down (insecurely), or both [26-28].

This leads us to the conclusion that good passwords are long, but at the same time hard to remember. Thus, conforming to one aspect of password management policy (good and strong passwords) leads the user not to conform to the aspect of memorability (do not write the password down).

The problem we are addressing in our research is how strictness of password policies regarding the password length is affecting memorability of passwords selected under such policies.

B. Related work – password types

Typically, a user is authenticated based on one of the three underlying principles (or combinations thereof): “what you know”, “what you are” and “what you have” [31, 32]. What-you-are (biometric) and What-you-have (tokens, smart physical objects) are not a part of this study as the authentication scheme is very different.

The passwords that are generated based on “what you know” principle can be divided into textual passwords and graphical passwords [33-35]. In our contribution we focus on textual passwords as graphical ones require a different user interface for entering passwords [34] and are thus not directly comparable to our study. Interestingly, it was already shown that some forms of graphical passwords can be attacked using automated tools [36].

The strongest passwords by far are those randomly selected, but they are at the same time the hardest to remember and thus subject to unsafe practices [32]. There are several “what-you-know” alternatives to a (nearly) random long textual password.

First, a password can be based on personal data or characteristics (e.g. birthdate, names, pets, addresses, etc.). They are easy to be cracked [1, 37] and their use is strongly discouraged [38]. Second, cognitive password authentication schemes require user to answer a randomly selected set of personal questions which only an authorized user can answer correctly. They have a high recall rate, but are susceptible to guesses by family and friends [21]. To prevent reuse, each authenticating system would require a unique set of questions [39]. Third, pass-sentences and pass-phrases are passwords composed of long, grammatically correct phrases [40]. They are memorable and software-cracking resistant, but their length makes them useless for repeated use [39], especially on the mobile devices. Fourth, randomly generated but pronounceable passwords made up of concatenated pronounceable syllables are resistant to standard dictionary or brute-force attacks [41], but the algorithm is vulnerable to a special dictionary attack [42]. Fifth, mnemonic passwords are those where a user chooses a memorable phrase and uses a character – often the first letter – to represent each word in the phrase, or vice versa, for a given (random) passphrase a system generates a grammatically correct phrase that the user can remember. They were endorsed in the past [15], but were found vulnerable and will even be more vulnerable in the future [21], although users tend to remember them more easily [43]

Cipresso and colleagues have proposed a novel method for generating textual passwords [44], and improved in [24]. "*The idea of PsychoPass is that a password can be created, memorized and recalled by just thinking of an action sequence instead of a word or string of characters*" [44]. The user thus memorizes a password based on its visual representation (action sequence) and additionally when to press SHIFT or ALT-GR. A detailed discussion on the strength of the psychopass passwords can be found in [23].

Orthogonal to the works on different textual password generating techniques are contributions that deal with password metrics, principally meters that show users how strong their password might be [17, 45, 46]. It was shown empirically [45] and mathematically [47] that Shannon entropy value is not useful when determining the strength of a password creation policy, and other policies need to be used. Common advices on minimum password length and character set requirements provide against online attacks [45]. Yet, by observing these requirements, users tend to forget passwords and/or write them down, usually in an insecure location [37]. Writing down a password is not a bad practice itself, as pointed out by Bruce Schneier: "*…if only users wrote [a password] down on a small piece of paper, and keep it with their other valuable small pieces of paper: in their wallet*" [48].

C. Related work – password management policies

A good summary of standardized password policies is presented in [49]. The U.S. National Institute of Standards and Technology published a Guide to enterprise password management, publication 800-118 [50], which defines four authentication assurance levels (AAL). For each level, several password management policy elements must be implemented. These elements address a) the required password length, b) required type and number of used character sets (e.g. lower/uppercase letters, numerals, special characters), c) password composition restrictions, d) password change frequency, e) technical password management (related to storing and transmitting of passwords), f) password management restrictions, and g) password origin.

A strict password management policy requires:

a) password length: minimum 8 characters
b) type and number of used character sets: (type): at least upper and lower case plus one numeral or a special symbol; (number): at least three
c) composition restrictions: no biographic elements, no dictionary words
d) password change frequency: at least in 12 months
e) technical password management: no stored passwords allowed (only salted hashes), no password transmission over insecure networks
f) management restrictions: password reuse not allowed, writing down of passwords not allowed, deriving passwords from other passwords is not allowed
g) password origin: system-assigned

A very strict password management policy thus assigns a minimum 8-character, mixed upper and lowercase plus numeral plus special character, not in a dictionary password [23]. The element on management restriction relies on a user and is very hard to implement, despite abundant training [7].

D. The contribution and organization of the paper

The aim of our research is twofold: (1) to find out whether users remember passwords under very strict password management policies and (2) to present the findings on using the improved PsychoPass method for creation of strong passwords with respect to the memorability.

We test the following working hypotheses: (1) there is no difference in recall for all types of passwords under very strict password management policy, and (2) the PsychoPass password is easier to remember than other types of password after a certain period of time has passed. Both hypotheses were tested under a condition that a user must comply with a strict password creation policy, requiring the user to select one of the (safe/good/strong) passwords proposed by the system.

In Section 2, we present the experimental methods used in our research, describe data collection and processing and elaborate on hypotheses in detail. In Section 3, we present the results of the analyses and in Section 4 we give a discussion on the results and conclude the work.

II. METHODS

The traditional password creation methods and the PsychoPass method was tested on a group of second year computer science students (*n*=45) at University of Maribor, Faculty of Electrical Engineering and Computer Science (Slovenia, Europe) by using a specially developed web tool, available on-line[1]. The experiment was designed so that each student was assigned three passwords of different types: a password with randomly selected characters (random

[1] http://studentwebserver.informatika.uni-mb.si/PassTest/?lang=en; for testing purposes a default username "demo" and password "demo" is available

password), a password by using concatenations of words and numbers (mnemonic password), and a PsychoPass password.

The emulated strict password management policy required the user to select a password made of randomly selected 8 characters, a 14-letter randomly generated mnemonic password (word-digits-word) and an 11-character randomly generated Psychopass password. Different lengths accounted for differences in password types; each such password is comparable in strength to the other.

When a student has logged in to the experimental web page, the system has displayed a randomly generated password. If the student did not like the assigned password, an alternative was offered. This way we emulated a strict password policy which does not allow a user to select her own and possibly a weak password. Once the password was accepted, the user was re-typing the assigned password back to the system for two minutes for the random and mnemonic, and for five minutes for the psychopass password. The allowed time for entering the repetitions was determined in the testing phase of the web page by external evaluators. The selected password was stored in a database with user's details. The time needed for typing the password was measured and whether the re-types of the password were correct or not.

The experiment was repeated in one week. This time it was checked if a student had remembered any of the assigned passwords. The students had a possibility to enter the password correctly three times only (simulating a real-world lockout). If she or he did not remember it, the system had it displayed for the user's reference.

A. Data collection and processing

The data from the experiment and its web page were collected in a database. For each user a login username and password were initially stored. Additionally, the time taken to enter each password was measured for all the students. The data whether the typing was successful or not (i.e. the password was re-typed correctly) was collected as well. If the password was incorrectly entered, the clock was not reset until the next correctly entered password. From the collected data we removed 5 users' entries because they did not complete all three tests or they did not enter some of the passwords correctly at least once. The final dataset contains data from 40 users.

B. Hypotheses

We hypothesize that there is no relationship between the password type and the recall (remembrance) rate, and we expect that users forget passwords under very strict password management policies. Thus:

- Hypothesis 1: H_{0-1}: the remembrance rate is zero for all password types.

  Alternatively, if the rate is not zero, the remembrance rate is independent of password type (H_1).
- Hypothesis 2: H0-2: there is no association between the password type and the recall rate.

C. Statistical analysis

The data sets containing measurements of time needed to enter a password for the first time and for the last time in the given time frame for three different groups of measurements (group 1: random, group 2: mnemonic, group 3: psychopass) were analyzed using relevant tests. We considered differences to be significant at the $\alpha < 0.05$ level. SPSS version 21 (IBM Corporation, Armonk, NY, USA) was used for analysis.

III. RESULTS

The second (and the main) part of the experiment was implemented after one week from the first part. Here, the students were asked by the system to enter each of the three passwords that were assigned to them by a system a week ago. The results show that no one had remembered the random or mnemonic-based password (see Table 3), but surprisingly, 10 % of the students were able to remember their assigned psychopass password after one week. Thus, hypothesis H_{0-1} needs to be rejected.

The system log revealed that all of the users that remembered the password were successful only on the third try. Thus, we can conclude that users had it not written down; otherwise they would be right in the first try.

TABLE 3: THE RESULTS OF THE SECOND PART OF THE EXPERIMENT - REMEMBRANCE

	Random	Mnemonic	Psychopass
Did not remember	40	40	36
Did remember	0	0	4
Total	40	40	40

We have checked whether the better results in remembering the psychopass passwords are due to the chance alone or is there a systematic reason behind the ease of recall. The chi-square (χ^2) test for independence, also called Pearson's chi-square test or the chi-square test of association, would normally be used to discover if there is a relationship between the password type and recall. However, since there are empty cells, Fisher Exact test is used.

TABLE 4: THE RESULTS OF THE CHI-SQUARE AND FISHER EXACT TEST

	Value	df	Asymp. Sig. (2-sided)	Exact. Sig. (2-sided)
Pearson Chi-Square	8.276	2	0.016	
Fisher Exact Test	10.940	2	0.011	0.033
N of Valid Cases	120			

We can see from Table 4 that Fisher Exact test yields P value of P=0.033. Thus, the second null hypothesis H_{0-2} that the variables are independent can be rejected. In other words, there is a statistically significant association (at $\alpha < 0.05$ level) between password type and recall; that is, different types of passwords are not equally likely to be remembered and hence psychopass passwords are easier to remember (there is a significance association between password type and the remembrance rate). The observed frequency of remembered psychopass passwords is 2.9 standard errors higher than would be expected if there were no association between password type and remembrance. The level of association is moderately strong.

IV. DISCUSSION AND CONCLUSION

As expected, none of the persons taking part in the experiment remembered their randomly-generated password; neither did anyone remember the assigned mnemonic-based password. However, 10 % of persons did remember their PsychoPass password. There is a statistically significant association (P=0.016) between password type and recall, i.e. is the psychopass passwords are easier to remember; the level of association is moderately strong. The remembrance rate is non-zero only for Psychopass password. However, the rate itself is very low, meaning the strict password management policies are placing a very high burden on users' cognitive load.

Passwords are Achilles' heel of modern computing as they are mostly at users' responsibility. The computer community has not made a very much needed shift in password management for more than 35 years. It seems nothing has changed since Robert Morris and Ken Thompson wrote the seminal paper on (UNIX) password security in 1979: the passwords are still the main method of authentication [13-18] and the users and their passwords remain the weakest link [7-11].

It was observed that most common password creation policies remain vulnerable to on-line attacks and that external password creation policies need to be enforced [49], mainly due to a subset of users selecting passwords that comply with the password policy. For example, a password policy may require the use of mixed upper and lower case letters, at least one symbol and one digit, but the *»PassWord!1«* is nevertheless a weak one.

In our contribution we presented results of a study how users remember different types of passwords under a very strict password management policy. As expected, under very strict rules users forget the assigned passwords. Surprisingly, passwords created under PsychoPass method, proposed by Cipresso et al [53] and improved in [25], are more easily remembered by users. The remembrance is not due to chance; the method is systematically better.

The results of this study have shown that under strict password management policies the remembrance rate is extremely low for all types of passwords. This is relevant to applications where strict password management policies are enforced. In such settings, a password complying to a strict security policy is highly resilient and prevents several types of attacks, such as brute-force attacks (on- and off-line), dictionary attacks and probable password attacks (e.g. Markov-model based). The benefit of a strong password is offset by a low remembrance rate, which in turn increases vulnerabilities in user management restrictions, such as no-write-down policy and no-reuse policy. These restrictions are imposed on a user and hence the organization has no or little control over it, as the complying is completely at a user's responsibility, thus generating the weakest link in a security chain [10].

Overall, the passwords as such will have to be replaced by other authentication mechanisms in the long term.

REFERENCES

[1] Morris R and Thompson K. Password security: A case history. Commun. ACM 1979; 22(11): 594-597.

[2] Corbató FJ. On building systems that will fail. Communications of the ACM 1991; 34(9): 72-81. DOI: 10.1145/114669.114686.

[3] Kerber R. Cost of data breach at TJX soars to $256 m. in Boston Globe Available on-line at http://www.boston.com/business/globe/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m/?page=full. Accessed: 2014-08-27. (Archived by WebCite® at http://www.webcitation.org/6JBdAIRnP); 2007.

[4] Segall L. Pastor outed on Ashley Madison commits suicide. CNNMoney. p. September 8, 2015.

[5] PRC. Privacy Rights Clearinghouse. Chronology of Data Breaches. Security Breaches 2005 - Present 2014; Available from: http://www.privacyrights.org/data-breach. Accessed: 2014-10-20. (Archived by WebCite® at http://www.webcitation.org/6AfYySWJK).

[6] Brown AS, Bracken E, Zoccoli S and Douglas K. Generating and remembering passwords. Applied Cognitive Psychology 2004; 18(6): 641-651. DOI 10.1002/acp.1014.

[7] Adams A and Sasse MA. Users are not the enemy. Communications of the ACM 1999; 42(12): 40-46. DOI: 10.1145/322796.322806.

[8] Adams A, Sasse MA and Lunt P. Making passwords secure and usable. People and Computers XII, chapter 1. . London: Springer London; 1997. p. 1-19. ISBN: 3540761721

[9] Notoatmodjo G. Exploring the 'Weakest Link': A Study of Personal Password Security. MSc Thesis. The University of Auckland, New Zealand; 2007.

[10] Sasse MA, Brostoff S and Weirich D. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. BT technology journal 2001; 19(3): 122-131. DOI: 10.1023/A:1011902718709.

[11] Tam L, Glassman M and Vandenwauver M. The psychology of password management: a tradeoff between security and convenience. Behaviour & Information Technology 2009; 29(3): 233-244. DOI 10.1080/01449290903121386.

[12] Oprea L. Unveilling the Password Encryption Process under Windows - A Practical Attack Proceedings of the Romanian Academy, Series A 2013; 14(Special Issue 2013): 317–327.

[13] Loch KD, Carr HH and Warkentin ME. Threats to information systems: today's reality, yesterday's understanding. MIS Quarterly 1992; 16(2): 173-186. DOI: 10.2307/249574.

[14] Tzong-Chen W and Hung-Sung S. Authenticating passwords over an insecure channel. Computers & Security 1996; 15(5): 431-439. DOI: 10.1016/0167-4048(96)00004-1.

[15] Zviran M and Haga WJ. Cognitive passwords: the key to easy access control. Computers & Security 1990; 9(8): 723-736. DOI: 10.1016/0167-4048(90)90115-A.

[16] Lee C-C, Liu C-H and Hwang M-S. Guessing Attacks on Strong-Password Authentication Protocol. International Journal of Network Security 2013; 15(1): 64-67.

[17] Egelman S, Sotirakopoulos A, Muslukhov I, Beznosov K and Herley C. Does my password go up to eleven?: the impact of password meters on password selection. Proceedings of the 2013 SIGCHI Conference on Human Factors in Computing Systems; 2013. April 27 - May 2, Paris, France: ACM.

[18] Creese S, Hodges D, Jamison-Powell S and Whitty M. Relationships between Password Choices, Perceptions of Risk and Security Expertise. Human Aspects of Information Security, Privacy, and Trust. First International Conference, HAS 2013, Held as Part of HCI International

2013. Las Vegas, NV, July 2013. Springer; 2013. p. 80-89. ISBN: 3642393446

[19] Al-Hudhud G, Abdulaziz Alzamel M, Alattas E and Alwabil A. Using brain signals patterns for biometric identity verification systems. Computers in Human Behavior 2014; 31(0): 224-229. DOI 10.1016/j.chb.2013.09.018.

[20] Jiang P, Wen Q, Li W, Jin Z and Zhang H. An Anonymous User Authentication with Key Agreement Scheme without Pairings for Multiserver Architecture Using SCPKs. The Scientific World Journal 2013; 2013(Article ID 419592). DOI 10.1155/2013/419592.

[21] Kuo C, Romanosky S and Cranor LF. Human selection of mnemonic phrase-based passwords. Proceedings of the second symposium on Usable privacy and security, July 12-14; 2006. Carnegie Mellon University, Pittsburgh, PA, USA: ACM.

[22] Liaojun P, He L, Pei Q and Wang Y. Secure and efficient mutual authentication protocol for RFID conforming to the EPC C-1 G-2 standard. in 2013 IEEE Wireless Communications and Networking Conference (WCNC)Shanghai, China: IEEE; 2013. p. 1870-1875.

[23] Brumen B and Černezel A. Brute force analysis of PsychoPass-generated Passwords. in 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)Opatija, Croatia, 26-30 May 2014; 2014. p. 1366-1371.

[24] Brumen B, Heričko M, Rozman I and Hölbl M. Security Analysis and Improvements to the PsychoPass Method. Journal of Medical Internet Research 2013; 15(8): e161. DOI 10.2196/jmir.2366; PMID: 23942458.

[25] Florencio D and Herley C. A large-scale study of web password habits. Proceedings of the 16th international conference on World Wide Web; 2007. ACM.

[26] Yan J, Blackwell A, Anderson R and Grant A. The memorability and security of passwords: some empirical results. in Technical report # UCAM-CL-TR-500.Cambridge, UK: University Of Cambridge; 2000.

[27] Yan J, Blackwell A, Anderson R and Grant A. Password Memorability and Security: Empirical Results. IEEE SECURITY & PRIVACY 2004; 2(5): 25-31. DOI: 10.1109/MSP.2004.81.

[28] Zviran M and Haga WJ. A comparison of password techniques for multilevel authentication mechanisms. The Computer Journal 1993; 36(3): 227-237.

[29] Miller GA. The magical number seven, plus or minus two: some limits on our capacity for processing information. Psychological review 1956; 63(2).

[30] Johnson GJ. A distinctiveness model of serial learning. Psychological review 1991; 98(2): 204-217. DOI: 10.1037/0033-295X.98.2.204.

[31] Stallings W. Cryptography and Network Security: Principles and Practices. 4th ed.Upper Saddle River, NJ: Prentice-Hall; 2006. ISBN: 0131873164

[32] Pfleeger CP and Pfleeger SL. Security in computing. 3rd ed.Upper Saddle River, NY, USA: Prentice Hall PTR; 2003. ISBN: 0130355488

[33] Davis D, Monrose F and Reiter MK. On User Choice in Graphical Password Schemes. USENIX 2004 Security Symposium; 2004.

[34] Suo X, Zhu Y and Owen GS. Graphical passwords: A survey. in 21st Annual Computer Security Applications ConferenceTucson, AZ, USA: IEEE; 2005. p. 463-472.

[35] Birget JC, Dawei H and Memon N. Graphical passwords based on robust discretization. Information Forensics and Security, IEEE Transactions on 2006; 1(3): 395-399. DOI: 10.1109/TIFS.2006.879305.

[36] Van Oorschot PC, Salehi-Abari A and Thorpe J. Purely Automated Attacks on PassPoints-Style Graphical Passwords. Information Forensics and Security, IEEE Transactions on 2010; 5(3): 393-405. DOI: 10.1109/TIFS.2010.2053706.

[37] Zviran M and Haga WJ. Password security: an empirical study. Journal of Management Information Systems 1999; 15: 161-186.

[38] FIPS. PUB 112 Password Usage. National Institute of Standards and Technology; 1985. ISBN:

[39] Brostoff AS. Improving Password System Effectiveness. PhD Thesis, Department of Computer Science, University College London. London, UK: University of London; 2004.

[40] Spector Y and Ginzberg J. Pass-sentence- a new approach to computer code. Computers & Security 1994; 13(2): 145-160. DOI: 10.1016/0167-4048(94)90064-7.

[41] Gasser M. A Random Word Generator for Pronounceable Passwords, MTR-3006. ESD-TR-75-97, AD-A017676. Bedford, Mass: MITRE Corp.; 1975. ISBN:

[42] Ganesan R, Davies C and Atlantic B. A new attack on random pronounceable password generators. Proceedings of the 17th {NIST}-{NCSC} National Computer Security Conference; 1994. Baltimore, MD, USA.

[43] Nelson D and Vu K-PL. Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords. Computers in Human Behavior 2010; 26(4): 705-715. DOI 10.1016/j.chb.2010.01.007.

[44] Cipresso P, Gaggioli A, Serino S, Cipresso S and Riva G. How to Create Memorizable and Strong Passwords. Journal of Medical Internet Research 2012; 14(1): e10. . DOI 10.2196/jmir.1906. PMID: 22233980

[45] Weir M, Aggarwal S, Collins M and Stern H. Testing metrics for password creation policies by attacking large sets of revealed passwords. Proceedings of the 17th ACM conference on Computer and communications security; 2010. Chicago, IL, USA: ACM.

[46] Bishop M and Klein DV. Improving system security via proactive password checking. Computers & Security 1995; 14(3): 233-249. DOI: 10.1016/0167-4048(95)00003-Q.

[47] Verheul ER. Selecting secure passwords. Topics in Cryptology–CT-RSA 2007. . Springer; 2006. p. 49-66. ISBN: 3540693270

[48] Schneier B. Write Down Your Password. in Schneier on Security. June 17, 2005 Available at http://www.schneier.com/blog/archives/2005/06/write_down_your.html. Accessed: 2014-08-30. (Archived by WebCite® at http://www.webcitation.org/6JEOK0Vdl); 2005.

[49] AlFayyadh B, Thorsheim P, Jøsang A and Klevjer H. Improving usability of password management with standardized password policies. The Seventh Conference on Network and Information Systems Security—SAR-SSI; 2012.

[50] Scarfone K and Souppaya M. Guide to enterprise password management (draft). NIST Special Publication 2009; 800: 118.