Volume 8 ▪ Issue 1 ▪ February 2014

INTERNATIONAL JOURNAL OF SECURITY (IJS)

ISSN : 1985-2320

Publication Frequency: 6 Issues / Year

CSC PUBLISHERS
http://www.cscjournals.org

INTERNATIONAL JOURNAL OF SECURITY (IJS)

VOLUME 8, ISSUE 1, 2014

EDITED BY
DR. NABEEL TAHIR

ISSN (Online): 1985-2320

International Journal of Security (IJS) is published both in traditional paper form and in Internet. This journal is published at the website http://www.cscjournals.org, maintained by Computer Science Journals (CSC Journals), Malaysia.

IJS Journal is a part of CSC Publishers
Computer Science Journals
http://www.cscjournals.org

INTERNATIONAL JOURNAL OF SECURITY (IJS)

Book: Volume 8, Issue 1, February 2014
Publishing Date: 11-02-2014
ISSN (Online): 1985-2320

IJS Journal is a part of CSC Publishers
http://www.cscjournals.org

Typesetting: Camera-ready by author, data conversation by CSC Publishing Services – CSC Journals, Malaysia

CSC Publishers, 2014

EDITORIAL PREFACE

This is the First Issue of Volume Eight of The International Journal of Security (IJS). The Journal is published bi-monthly, with papers being peer reviewed to high international standards. The International Journal of Security is not limited to a specific aspect of Security Science but it is devoted to the publication of high quality papers on all division of computer security in general. IJS intends to disseminate knowledge in the various disciplines of the computer security field from theoretical, practical and analytical research to physical implications and theoretical or quantitative discussion intended for academic and industrial progress. In order to position IJS as one of the good journal on Security Science, a group of highly valuable scholars are serving on the editorial board. The International Editorial Board ensures that significant developments in computer security from around the world are reflected in the Journal. Some important topics covers by journal are Access control and audit, Anonymity and pseudonym, Computer forensics, Denial of service, Network forensics etc.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Starting with Volume 8, 2014, IJS appears in more focused issues. Besides normal publications, IJS intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

The coverage of the journal includes all new theoretical and experimental findings in the fields of computer security which enhance the knowledge of scientist, industrials, researchers and all those persons who are coupled with computer security field. IJS objective is to publish articles that are not only technically proficient but also contains information and ideas of fresh interest for International readership. IJS aims to handle submissions courteously and promptly. IJS objectives are to promote and extend the use of all methods in the principal disciplines of computer security.

IJS editors understand that how much it is important for authors and researchers to have their work published with a minimum delay after submission of their papers. They also strongly believe that the direct communication between the editors and authors are important for the welfare, quality and wellbeing of the Journal and its readers. Therefore, all activities from paper submission to paper publication are controlled through electronic systems that include electronic submission, editorial panel and review system that ensures rapid decision with least delays in the publication processes.

To build its international reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJS. We would like to remind you that the success of our journal depends directly on the number of quality articles submitted for review. Accordingly, we would like to request your participation by submitting quality manuscripts for review and encouraging your colleagues to submit quality manuscripts for review. One of the great benefits we can provide to our prospective authors is the mentoring nature of our review process. IJS provides authors with high quality, helpful reviews that are shaped to assist authors in improving their manuscripts.

Editorial Board Members
International Journal of Security (IJS)

EDITORIAL BOARD

TABLE OF CONTENTS

Volume 8, Issue 1, February 2014

Pages

Password Security

Danuvasin Charoen *danuvasin@nida.ac.th*
NIDA Business School
National Institute of Development Administration
Bangkok, 10240, Thailand

Abstract

This study investigates users' behavior in password utilization. Good password practices are critical to the security of any information system. End users often use weak passwords that are short, simple, and based on personal and meaningful information that can be easily guessed. A survey was conducted among executive MBA students who hold managerial positions. The results of the survey indicate that users practice insecure behaviors in the utilization of passwords. The results support the literature and can be used to guide password management policy.

Keywords: Password Security, Password Utilization, Password Management.

1. INTRODUCTION

Although there are currently many forms of authentication methods, such as biometric and smartcard, the most common method for authentication is the combination of user ID (identification) and password (authentication). The following section describes the two steps of the authentication process using passwords (Sasse, Brostoff, & Weirich, 2001).

1.1 User ID and Password (Sasse et al., 2001)

First, users are either assigned an ID or are given the chance to create one. Once the ID has been created, the user chooses a password. The password should be secret and shared only between the user and the information systems or computer. Users should not disclose their passwords or write them down.

1.2 Log-on (Sasse et al., 2001)

During the login process, users must enter both their user IDs and passwords. The system then processes and compares the ID and password with what is stored in the database. If the user ID and password match, the user will be granted access to the system. If the user ID and password do not match, the user will not be allowed access. Many information systems suspend a user account after three to five unsuccessful login attempts. The users must then visit a system administrator to reset the password.

Since 1970, instead of storing all passwords in a file, passwords have been stored in a cryptographic hash (Schneier, 2000). When the user types her password into a computer, website, or software application, the software calculates the hash of the password and compares it with the hash stored in the file (Schneier, 2000). If they match, the user is allowed in (Schneier, 2000). However, if a cracker has acquired a copy of the hashed password file, the cracker can use a dictionary to compute the hash of every word in the dictionary (Schneier, 2000). If the hash word matches a password entry, then the cracker obtains a password (Schneier, 2000). If a cracker has tried all the words in a dictionary and remains unsuccessful, he or she will try reversing dictionary words, capitalizing letters, etc. (Schneier, 2000). Finally a cracker will try all character combinations (Schneier, 2000).

1.3 Password Standards

The following sections describe the characteristics of strong and weak passwords according to the Sans Institute Password Policy (Sans.org, 2013).

Characteristics of Weak Passwords (Sans.org, 2013)

1. The password has less than fifteen characters.
2. The password is a word that can be found in a dictionary (English or foreign).
3. The password is an ordinary word such as
    a. Names of family, pets, friends, co-workers, fantasy characters, etc.
    b. Computer terms or names, commands, sites, companies, hardware, software.
    c. The words "<Company Name>", "sanjose", "sanfran" or any similar derivation.
    d. Birthdays and other personal information such as addresses and phone numbers.
    e. Word or number patterns such as aaabbb, qwerty, zyxwvuts, 123321, etc.
    f. Any of the above spelled backwards.
    g. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

1.4 A Strong Passwords has the Following Characteristics (Sans.org, 2013):

1. Contains both upper and lower case characters (e.g., a-z, A-Z)
2. Contains numbers and symbols as well as letters, for example, 0-9,!@#$%^&*()_+|~ =\‘{}[]:";’<>?,./)
3. Contains at least fifteen alphanumeric characters.
4. Is not a word in any language, slang, dialect, jargon, etc.
5. Is not based on personal, meaningful information such as names of family, telephone number, SSN, etc.
6. Is never be written down or stored on-line.

In sum, a good password should be complex but nevertheless easy to remember (Burnett, 2002). A good password should also be long and consist of letters, numbers, and symbols. It should let the user type quickly with few errors (Burnett, 2002). Most importantly, a good password should appear random yet be familiar and meaningful to the user (Burnett, 2002). The best password policy is the one that enables the user to create these passwords (Burnett, 2002). However, the recommendations of most password policies are not always practiced by users or enforced (B.DawnMedlin & Cazier, 2005).

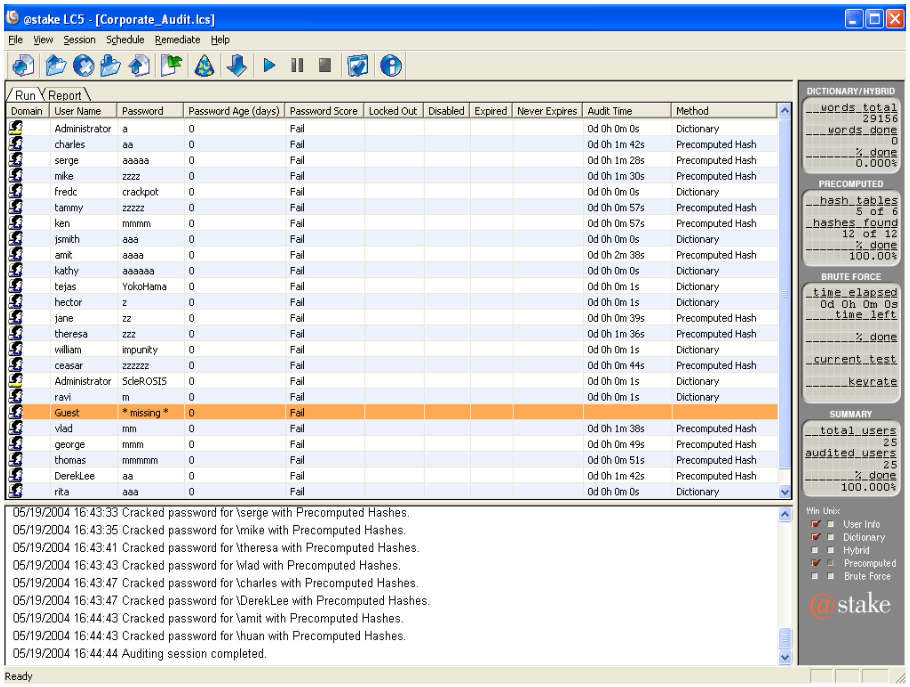
1.5 How Secure Are Passwords?

The measure of disorder is called entropy (Schneier, 2000). In other words, the more entropied something is, the more uncertainty there is in that particular thing (Schneier, 2000). For instance, if we choose a random person from any population, we will choose either male or female (Schneier, 2000). That indicates that the gender variable has one bit of entropy (Schneier, 2000).

Most people who create cryptographic algorithms consider 128 bits to be strong (Schneier, 2000); however, this is not the same thing as entropy (Schneier, 2000). This is because 128 bits is not a measure of randomness, but the key length that measures the maximum amount of work that a hacker or cracker must do to break the algorithm and obtain the key (Schneier, 2000). One hundred and twenty-eight bits indicates nothing about the minimum (Schneier, 2000).

Most keys are generated from passphrases or passwords (Schneier, 2000). An information system that accepts 10-character ASCII passwords has 80 bits to represent; however, it has less than 80 bits of entropy (Schneier, 2000). Standard English has approximately 1.3 bits of entropy per character (Schneier, 2000). A password with 8 characters has the same entropy as a 32-bit key length (Schneier, 2000). Thus, to arrive at a 128-bit key length, an English-speaking individual would be required to use a 98-character passphrase (Schneier, 2000). Notably, Windows' algorithms, which its designers consider to be quite strong, accept a 128-bit key length (Schneier, 2000). However, the entropy in the password is far lower than that (Schneier, 2000).

Password-cracking software will not try every possible key in order (Schneier, 2000). It will try the most likely password first and then try the rest based on probability (Schneier, 2000). For instance, a brute force password- cracking software in figure 1 will try common passwords such as "password," "admin," or "1234" first; then it will try the entire English dictionary; and then varied capitalization, numbers, and other symbols (Schneier, 2000). The program described in the previous section is called L0phtcrack.



Domain	User Name	Password	Password Age (days)	Password Score	Locked Out	Disabled	Expired	Never Expires	Audit Time	Method
	Administrator	a	0	Fail					0d 0h 0m 0s	Dictionary
	charles	aa	0	Fail					0d 0h 1m 42s	Precomputed Hash
	serge	aaaaa	0	Fail					0d 0h 1m 28s	Precomputed Hash
	mike	zzzz	0	Fail					0d 0h 1m 30s	Precomputed Hash
	fredc	crackpot	0	Fail					0d 0h 0m 0s	Dictionary
	tammy	zzzzz	0	Fail					0d 0h 0m 57s	Precomputed Hash
	ken	mmmm	0	Fail					0d 0h 0m 57s	Precomputed Hash
	jsmith	aaa	0	Fail					0d 0h 0m 0s	Dictionary
	amit	aaaa	0	Fail					0d 0h 2m 38s	Precomputed Hash
	kathy	aaaaaa	0	Fail					0d 0h 0m 0s	Dictionary
	tejas	YokoHama	0	Fail					0d 0h 0m 1s	Dictionary
	hector	z	0	Fail					0d 0h 0m 1s	Dictionary
	jane	zz	0	Fail					0d 0h 0m 39s	Precomputed Hash
	theresa	zzz	0	Fail					0d 0h 1m 36s	Precomputed Hash
	william	impunity	0	Fail					0d 0h 0m 1s	Dictionary
	ceasar	zzzzzz	0	Fail					0d 0h 0m 44s	Precomputed Hash
	Administrator	ScleROSIS	0	Fail					0d 0h 0m 1s	Dictionary
	ravi	m	0	Fail					0d 0h 0m 1s	Dictionary
	Guest	* missing *	0	Fail						
	vlad	mm	0	Fail					0d 0h 1m 38s	Precomputed Hash
	george	mmm	0	Fail					0d 0h 0m 49s	Precomputed Hash
	thomas	mmmmm	0	Fail					0d 0h 0m 51s	Precomputed Hash
	DerekLee	aa	0	Fail					0d 0h 1m 42s	Precomputed Hash
	rita	aaa	0	Fail					0d 0h 0m 0s	Dictionary

```
words total
29156
words done
0
% done
0.000%

hash tables
5 of 6
hashes found
12 of 12
% done
100.00%

time elapsed
0d 0h 0m 0s
time left

% done

current test

keyrate

total users
25
audited users
25
% done
100.000%
```

☑ □ User Info
☑ □ Dictionary
□ □ Hybrid
☑ □ Precomputed
□ □ Brute Force

```
05/19/2004 16:43:33 Cracked password for \serge with Precomputed Hashes.
05/19/2004 16:43:35 Cracked password for \mike with Precomputed Hashes.
05/19/2004 16:43:41 Cracked password for \theresa with Precomputed Hashes.
05/19/2004 16:43:43 Cracked password for \vlad with Precomputed Hashes.
05/19/2004 16:43:47 Cracked password for \charles with Precomputed Hashes.
05/19/2004 16:43:47 Cracked password for \DerekLee with Precomputed Hashes.
05/19/2004 16:44:43 Cracked password for \amit with Precomputed Hashes.
05/19/2004 16:44:43 Cracked password for \huan with Precomputed Hashes.
05/19/2004 16:44:44 Auditing session completed.
```

FIGURE 1: Example of password-cracking software from http://www.atstake.com/products/lc/images/lc5_screen_lrg.gif.

A dictionary-attack method such as L0phtcrack used to be difficult because computers were slow (Schneier, 2000) but is a lot easier now because computers today are much faster than those in the past (Schneier, 2000). For passwords with 7 characters in WindowNT, "L0phtcrack can try every alphanumeric password in 5.5 hours, every alphanumeric password with some common symbols in 45 hours, and every possible keyboard password in 480 hours" (Schneier, 2000, p. 137).

Moreover, Moore's Law has made it easy for a cracker to use the brute force method on long entropy keys (Schneier, 2000). Simultaneously, there is a maximum to the entropy of passwords that end users can or are willing to remember (Schneier, 2000). Considering that end users would have to memorize a 32-character random hexadecimal string to have a password equivalent to a 128-bit key (Schneier, 2000), it is not difficult to see why most people either opt for weaker passwords that are more easily memorizable or write them down.

2. LITERATURE REVIEW

2.1 Password Attributes

Zviran and Haga (1999) conducted a survey on computer users at a Department of Defense installation in California. Questionnaires were returned by 997 participants. Zviran and Haga (1999) observed that 24.9% of the respondents had 6 characters in their passwords.

Zviran and Haga (1999) also observed that 80.1% of the respondents' passwords consisted of only alphabetic characters.

Zviran and Haga (1999) observed that most user-selected passwords are derived from the characteristics of personal details meaningful to the individual, are fairly short, are made up of alphanumeric characters, are seldom changed, and are frequently written down. In other words, passwords remain easy to memorize and simple in structure and construction. Zviran and Haga (1999, p.179) observed the following:

1. Password selection methods affect password memorizability.

2. The increased frequency of changing a password, even though it increases the level of security, hinders memorizability.

3. The more frequently a password is used, the less often it is written down.

4. The more a password is used, the less difficult it is to remember.

5. Changing passwords frequently, although necessary to reduce password predictability, hinders recall.

6. Difficulty recalling a password is related to a user's tendency to write it down.

7. Difficulty recalling a password or writing it down is not related to a password's length.

8. Whether a password was chosen to make it easy to remember has no bearing on whether it is written down.

Zviran and Haga (1999) urge replication of their findings in future research to challenge these findings in various user populations and organizations to enhance their generalizability.

2.2 End User Security

When users are allowed to select their own passwords, they tend to select passwords that are easy to remember but also easy to crack (Adams & Sasse, 1999). End users prefer passwords that are short, simple, and derived from meaningful details (Adams & Sasse, 1999). Like Zviran and Haga (1999), Adams and Sasse (1999) observed that some users create their passwords based on details meaningful to them. This potentially includes variations of their own or a relative's name, a pet's name, street address, birth date, social security number, etc. (Adams & Sasse, 1999). They also observed that user knowledge regarding secure password content is not sufficient (Adams & Sasse, 1999). Most end users do not know how to create a secure password, and they do not know how serious it can be if their passwords are compromised (Adams & Sasse, 1999).

Adams and Sasse (1999) posit that, without instruction from IT experts, end users often create their own rules for inventing passwords, which are thus often not secure. Passwords that can be derived from the dictionary (real words) are extremely easy to crack from a hacker's perspective (Adams & Sasse, 1999). Most users do not know how password cracking works (Adams & Sasse, 1999).

2.3 Using Passwords Multiple Times

Although password theft is a danger to the information system in which a password is compromised, password theft can also threaten other information systems (Ives, Walsh, & Schneider, 2004). Because many people have multiple password-protected accounts and they often reuse identical passwords repeatedly, hackers can more easily gain access to other accounts (Ives et al., 2004)

For example, if a hacker gains access to a poorly protected departmental file server and the passwords are compromised, those passwords can be used to gain access to a more securely protected corporate system (Ives et al., 2004). This is referred to as a "domino effect" (Ives et al., 2004). A domino effect is the result of one site's password file being compromised by a hacker who then uses it to penetrate other information systems (Ives et al., 2004).

2.4 Organizational Problems

There is a major gap between end users and IT experts (Adams & Sasse, 1999). End users do not understand security issues whereas IT security departments do not understand end users' perceptions, tasks, and needs (Adams & Sasse, 1999). That is why IT departments view end users as security risks who need to be managed and controlled. Users may be perceived as the enemy within (Adams & Sasse, 1999). Conversely, users view security mechanisms as laborious overhead that can get in the way of their work (Adams & Sasse, 1999). Adams and Sasse (1999) also observed that an organization sometimes advocates the sharing of passwords to maximize convenience in the work process.

2.5 Social Problems

Sasse et al (2001) observed that sharing passwords is considered a sign of trust among colleagues and friends. People who are not willing to share passwords with colleagues are regarded as "untrusting" (Sasse et al., 2001). Users who practice safe computing by having strong passwords are often described as "paranoid" or "antisocial" (Sasse et al., 2001).

The following table summarizes the literature review related to end-user behavior in the utilizations of passwords:

Study	Regarding the study	Method	Results
Zviran, M., and Haga, W.J. "Password security: An empirical study," Journal of Management Information Systems (15:4) 1999, p. 161 (125 pages).	The paper addresses the gap in evaluating the characteristics of real-life passwords and presents the results of an empirical study on password use. The paper investigates the core characteristics of user-generated passwords and associations among those characteristics.	The researchers conducted questionnaires on computer users at the Department of Defense in California. Users returned 997 questionnaires.	1 Password selection methods affect password memorizability. 2. The frequency of changing a password hinders memorizability. 3. The more frequently a password is used, the less often it is written down. 4. The more a password is used, the less difficult it is to remember. 5. Changing passwords frequently hinders recall. 6. Difficulty recalling a password is related to a user's tendency to write it down. 7. Difficulty recalling a password or writing it down is not related to a password's length. 8. Whether a password was chosen in such a manner as to make it easy to remember is not related to whether it was written down.
Ives, B., Walsh, K.R., and Schneider, H. "The Domino Effect of Password Reuse," *Association for Computing Machinery. Communications of the ACM* (47:4) 2004.	The researchers analyze the problems of utilizing the same password multiple times (the domino effect) among the users.	The researchers use secondary data from other studies.	1. Many people have multiple password-protected accounts, and they often reuse the same passwords repeatedly. 2.If hackers can gain access to one account, they may be able to gain access to other accounts.
Adams, A., and Sasse, M.A. "Users are not the enemy," *Association for Computing Machinery. Communications of the ACM* (42:12) 1999, p. 40 (47 pages).	The study analyzes the issues related to password behaviors among end users.	The researchers conducted grounded theory in two organizations in the construction business to analyze the issues related to the user sides of	1. Many users need to remember too many passwords. 2. When the user cannot remember multiple passwords, the common solution is to write them down. 3. User knowledge regarding secure password content is not adequate. 4. IT departments view end users as security risks who must be managed and controlled. 5. Users view security mechanisms as laborious interferences with their work.

		password security. The researchers used web-based questionnaires and followed up with semi-structured in-depth interviews.	
Sasse, M.A., Brostoff, S., and Weirich, D. "Transforming the 'Weakest Link' -- a Human/Computer Interaction Approach to Usable and Effective Security," *BT Technology Journal* (19:3) 2001, p. 122.	The researchers investigated the behaviors of users regarding the use of passwords. The researchers concluded that undesirable behaviors associated with the use of passwords originate from the failure to understand the attributes of memorizability, incompatible task demands, and lack of training, support, and proper motivation.	The researchers conducted a qualitative study using questionnaires and in-depth interviews among users.	1. The frequency of using passwords can positively affect memorizability. 2. Passwords that require100% accurate recall are not good for infrequently used systems. 3. Heavily or frequently used passwords are more regularly confused than infrequently used passwords. 4. Recalling robust passwords that are rare or non-meaningful is an impossible task for humans. 5. People who have a strong password are viewed as “paranoid” or “antisocial”. 6. Sharing passwords is considered a sign of trust among colleagues and friends. 7. Most users underestimate the potential damage caused by compromised. passwords.
Warkentin, M., Davis, K., and Bekkering, E. "Introducing the Check-Off Password System (COPS): An Advancement in User Authentication Methods and Information Security," *Journal of Organizational and*	The study proposes that the Check off Password System (COPS) is more secure than self-selected passwords. The study analyzes	The researchers conducted a control experiment. There were 352 participants, all college students.	The study indicates that COPS is a better alternative to current user authentication method. The study suggests that end users perceive all password procedures tests to have equal usefulness; however, the perceived ease of use of the COPS method is equivalent to an established high security password, and the COPS interface does not negatively affect user performance compared with that of a high security password.

End User Computing (16:3) 2004, p. 41 (18 pages).	the differences between using COPS and three traditional password procedures.		

TABLE 1: Summary of Literature Review Regarding End User Behavior in the Utilizations of Passwords.

2.6 Memorizability

Miller (1956) indicates that human short-term memory can store only seven plus or minus two (7+/- 2) chunks or amounts of information. However, this rule applies to information that must be recalled without rehearsal (Hewett, 1999). Information can be memorized for a long period if it is rehearsed (Hewett, 1999; Newell & Simon, 1972).

In addition, Sasse, et al. (2001) note the following:

- The human memory is limited.
- Human memory can decay over time.
- Frequently used passwords are easier to memorize than less frequently used passwords.
- Humans cannot "forget on demand," which indicates that some items (passwords) are still in the memory even though they are not needed.
- Passwords that are meaningful are easier to remember than non-meaningful passwords.
- Different items can be related to one another to assist recall. Nonetheless, related or similar items can compete with one another for recollection.

Adams and Sasse (1999) observed that users' having many passwords can affect the passwords' memorizability. When users are assigned a cryptographically strong password such as "Da*3?^43jC", they will forget it; thus, they tend to write it down (Warkentin, Davis, & Bekkering, 2004). In addition, currently, end users must remember too many passwords. The evolution of e-commerce has resulted in a massive increase in the number of passwords required by end users (Ives et al., 2004).

When the user cannot remember every password, he or she will generally write them all down, which, of course, is considered an insecure practice because the passwords can be stolen or lost more easily.

2.7 Three Stages of Memory

According to Higbee (2001), there are three stages of memory:

1. Acquisition or encoding is learning or studying the material in the first place, or as Anderson defines it, "how a permanent representation of the information is encoded and how this record is strengthened" (Anderson, 1994, p. p.191). In the case of passwords, the acquisition process occurs when the users construct the passwords or they are assigned to the users in the first place.
2. Storage is keeping the material until it is needed. Storage, or retention, is "how the information is maintained in memory" (Anderson, 1994, p. p.191). In the case of passwords, the storage process occurs when the users memorize the passwords.
3. Retrieval is identifying the material and getting it back out when it is needed. Retrieval is "how the information is brought out of memory when needed" (Anderson, 1994, p. p.191). In the case of passwords, the retrieval process occurs when the user recalls the passwords.

2.8 Short-Term Memory

In general, most people cannot remember more than 7 digits (Higbee, 2001). A few people can remember 10 or 11 digits (Higbee, 2001), and a very few people can remember more than 11 digits (Higbee, 2001). Short-term memory refers to "how many items can be perceived at one time or how much a person can consciously pay attention to at once" (Higbee, 2001, p. 19). If the person does not have a systematic manner in which to memorize information, information stored in short-term memory is forgotten in less than 30 seconds (Higbee, 2001). That suggests that when a person acquires his or her password, the decay process is already occurring. However, the typical method of preventing this is rehearsal, which can serve two purposes: 1) it can retain the information in short-term memory or 2) it can help people transfer the information into long-term memory by giving them time to code it (Higbee, 2001). The rehearsal in the case of passwords is the frequency of use and is a component of the training mentioned in Chapter 4.

2.9 Long Term Memory

According to Higbee (2001), there are three types of long-term memory:

1. Procedural memory, or how one memorizes how to do something (skills such as typing);

2. Semantic memory, or how one memorizes factual information (such as math equations or word meanings) or in our case, password memorization;

3. Episodic memory, or how one memorizes personal events (such as a person's first date or where someone learned a particular equation).

The following diagram describes how memory works and the relation between short-term and long-term memory based on Atkinson and Shiffrin's theory:

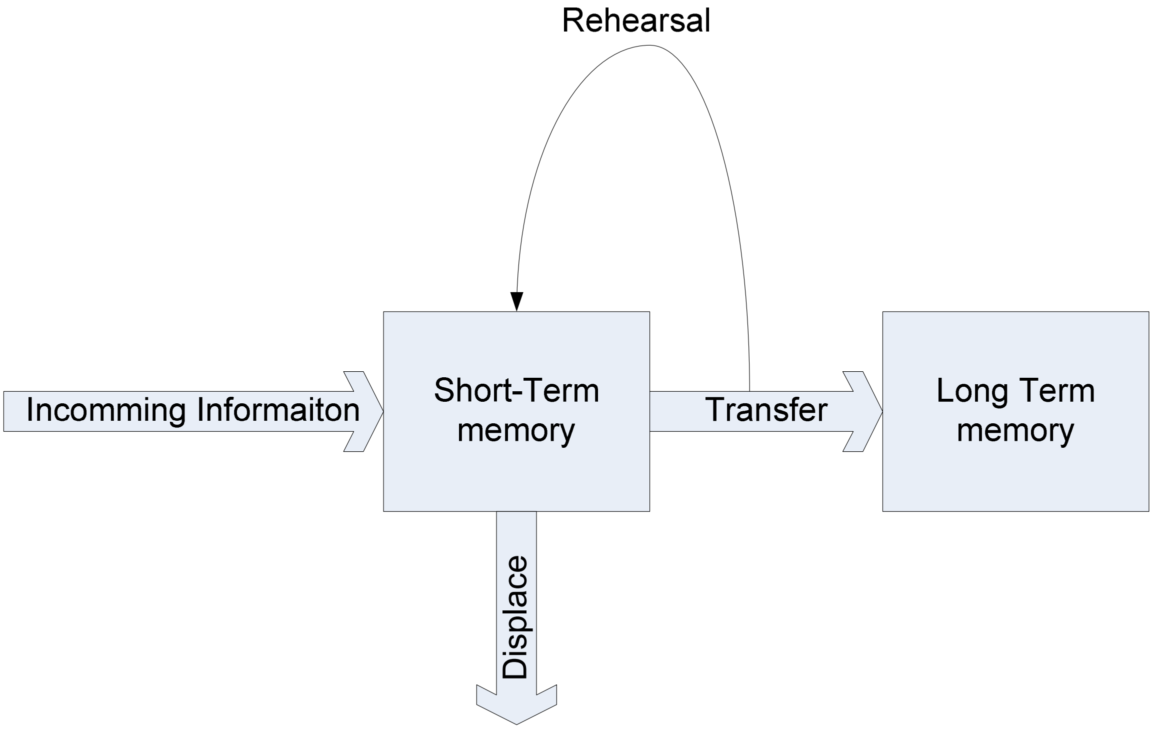


FIGURE 2: The Atkinson and Shiffrin (1968) theory regarding short-term and long-term memory.

The challenge of this study is how to transfer a password from short-term memory to long-term memory. There are several techniques and strategies that can aid in this transfer. The techniques and strategies are mentioned in chapter 4.

2.10 Five Reasons People Forget (Higbee, 2001)

1. Decay. Materials are not used. In the case of passwords, forgetting the passwords is caused by not using them or using them infrequently.

2. Repression. Unpleasant or unacceptable memories can be deliberately forgotten. In the case of passwords, the users may simply refuse to memorize a password because they do not like the password policy or do not like the assigned password.

3. Distortion. People remember some things the way they want to remember them. In the case of passwords, people may create their own systems of remembering the passwords, and those new systems may distort their memorization.

4. Interference. Information people have learned in the past may interfere with their memory of something they have learned recently (proactive inhibition). In the case of passwords, old passwords may interfere with the memorization of a new password. Information people have learned recently may interfere with their memory of something they learned in the past (retroactive inhibition). In the case of passwords, the new passwords may interfere with the remembering of old passwords.

5. Cue dependency. Memory relies on identifying the right cue to retrieve what was memorized. In the case of passwords, recalling the passwords depends on identifying the right cues, such as questions and answers, to be able to recall them.

2.11 How Fast Do People Forget?

Research on memory indicates that a person does not forget at a steady rate, that most memory loss occurs after learning; the rate of forgetting slows down and levels off as time passes (Higbee, 2001). Hence, the largest amount of what people forget will occur shortly after they have learned the information (Higbee, 2001). That suggests that the highest rate of forgetfulness occurs right after people acquire their passwords. However, the exception to the rule is that material that is learned systematically or that is extremely important may be retained in the memory for a long time (Higbee, 2001). Consequently, if the person learns how to remember the password systematically and if the person perceives passwords as important, he or she will be able to remember them for a long time.

2.12 The Basic Foundation of Memorization (Higbee, 2001)

1. Meaningfulness. The more meaningful the material is, the easier it will be to learn and remember. In his experiment, Anderson (1994) observed that “subjects tend to remember the meaning of a text rather than its exact wording” (Anderson, 1994). For instance, words grouped into meaningful categories are easier to remember than words presented in meaningless order.

2. Familiarity. The more people know about a particular subject, the easier it is to learn new information about it. In the case of passwords, the old password is easier to recall than the new password.

3 Rhymes. Many people use a rhyme to help them remember information. An example of a rhyme is the Alphabet Song (“AB-CD-EFG . . .”).

4. Patterns. If people can discern a pattern, rule, or underlying principle in the material, they will likely be able to learn it more easily. To render information more meaningful, patterns serve to chunk the material so there is less to remember. If people can see a pattern, then all they must memorize is the pattern, which will allow them to generate the original material.

5. Organization. If the material is organized, it will be easier to memorize. The position of the material also plays a role in memorization. Research indicates that the order in which items are organized can affect how easy they are to learn and memorize.

6. Association. Association involves relating what people want to learn to something they already know. This method can be accomplished by analogy. For instance, people can associate their passwords with what they are already familiar with such as familiar numbers, dates, or specific events.

7. Repetition. Repetition is the frequency of using the passwords. Users can use the repetition method to improve the memorizability of passwords by frequently using their passwords or by rehearsal.

3. RESEARCH METHOD

The survey was used to analyze the current characteristics of users' behavior in utilizing their passwords.

4. FINDINGS

The survey was sent to executive MBA students at one of the AACSB accredited business schools in Thailand. Of 90 students, 63 responded to the survey. Of the respondents, 46 (73%) were female, 17 (27%) were male, and 63% (40 students) were between 26 and 30 years old. Nineteen per cent (12 students) were between 31-35 years old, and 37 students (37%) worked for a private company. Sixteen per cent were entrepreneurs, and 14% worked for the government. Ninety-five per cent mentioned that they had an account with the information systems in their workplace. When asked about the number of characters in their passwords, the majority (29%) had 8 characters, 10% had 9 characters, 15% had 10 characters, 12% had 11 characters, and 7% had fewer than seven characters in their passwords. Of the respondents, 11% had only numbers in their passwords, 30% had both characters and numbers in their passwords, and 17% had characters, numbers, and symbols in their passwords.

When asked how they had created their passwords, 33% of the respondents responded that they thought of some name or date that has personal significance for them such as the name or birth date of a family member. Some (28%) combined entire or partial names, dates, words, and numbers to create a string of characters that they could remember such as ”Jane2005” or ”mycode7”. Eleven per cent mentioned they would think of a word that is easy to remember, such as ”basketball” or ”accounting”. Only 10% mentioned that they would make up ”nonsense” strings of letters, numbers, and symbols such as ”T3%x&W9” or ”GhW4q$p”.

When asked how often they used their passwords to log in to the company's systems, more than half (65%) said that they logged in to the company's systems many times a day; 18% only logged in once a day. When asked how many systems they used (other than their company's system) that required a password, 40% reported using 4 systems, and 15% reported using five systems.

When asked how many distinct passwords they used for all systems, only one person reported using only one password for all systems, 29% used two passwords for all systems, and the majority (41%) used three passwords for all systems.

When asked if they had ever used their company's passwords for any other systems, 50% (30 users) admitted they used company's passwords for other systems such as email, social networking, and other website registration.

When asked if they ever wrote down their passwords or stored their passwords in their computers, 37% (15 users) admitted writing down or storing their passwords in the computer. In addition, when asked if anyone else used their written passwords, 28% (17 users) admitted allowing other people to use their written passwords.

Nearly half (43%) admitted that they have shared their company's passwords with friends or colleagues; 42% of the users reported changing their company's passwords because they suspected that the passwords had been compromised or guessed by someone else.

When asked how often they changed their passwords, more than half (51%) reported never changing their passwords, and 23% reported changing their passwords every three months.

5. DISCUSSION

Passwords are still one of the weakest links in information systems because people use weak passwords. According to the survey, nearly eighty percent of users have fewer than ten characters in their passwords, and more than half of the respondents reported having only characters in their passwords. With the current password-cracking software, these passwords are easy to crack in a matter of seconds. The results of this study also show that people often create passwords based on their personal information such as birthdates, citizen id, telephone number, and family members' names. These passwords can be easily guessed by friends and colleagues. Another problem that I observed in the results of this study is people often reuse passwords. Nearly everyone in the study reported that they have only between two and three passwords to access every account. This can lead to the domino effect problem in which the hacker can gain access using one password and then use the same passwords for other accounts. Sometimes, the hackers do not even need to hack the password. They can set up a website and ask users to register with a username and password. Some people will reuse the same password that they use with other accounts such as email, their company's systems, and e-banking accounts. Once the hacker has a user's password, he or she can use the same password with other systems including users' email and e-Banking account.

In this study, the results present the contrast between strong passwords and memorization. Miller (1956) posits that human short-term memory can store only seven plus or minus two chunks of information (Miller, 1956), and unless a person develops a systematic way to memorize that information, it will be forgotten in less than 30 seconds (Higbee, 2001). This finding is consistent with the research documents used in creating the study, indicating that the longer a password is, the more difficult it is to remember (Sasse et al., 2001; Schneier, 2000; Warkentin et al., 2004; Zviran & Haga, 1999). When the users cannot memorize the passwords, the solution is for them to write the passwords down. In this study, nearly half of the respondents indicated that they wrote down their passwords to aid their password memorizability.

Sharing passwords is common practice in IS organizations (Sasse et al., 2001). Passwords are supposed to be secret; thus, sharing them defeats the purpose of having them, making it next to impossible to verify who the users are in the system or to account for what went wrong with the system (Sasse et al., 2001). The main reason users share their passwords is for convenience. In this study, the results indicate that nearly half (43%) admitted that they have shared company passwords with friends or colleagues. Finally, the results indicate that most users never change their passwords. This can create a serious problem because most users do not know if their passwords have already been compromised. The hacker can use compromised passwords to access users' accounts without the users' knowledge.

6. CONCLUSIONS

Passwords are the first line of defense in any information system; however, their importance has been ignored by both practitioners and researchers. The literature related to password security indicates that a strong password that is long, complicated, and not derived from personal, meaningful details is difficult to remember and weak passwords that are short, simple, and derived from personal, meaningful details are easy to remember (Schneier, 2000; Warkentin et al., 2004; Zviran & Haga, 1999). When users cannot memorize a password, the solution is to write it down (Sasse et al., 2001; Schneier, 2000; Zviran & Haga, 1999). A written password can be lost or stolen. In addition, when users cannot memorize numerous passwords, they often reuse the same password multiple times. If hackers can gain access to one account, they may be able to gain access to other accounts (Ives et al., 2004). Memory literature indicates that humans have a limited capacity for memorizing information (Higbee, 2001; Miller, 1956). Information stored in long-term memory can be memorized for a longer period than information stored in short-term memory (Higbee, 2001). The findings of this study support previous findings in the literature that end users use weak passwords. The majority of users write down their passwords. Most users reuse a password for multiple accounts. Most users share their passwords and never change them. IT security must develop both technical and policy solutions to address the problems of users' behavior in utilizing passwords; otherwise, passwords will continue to be a weak link in information systems.

7. REFERENCES

[1] Adams, A., & Sasse, M. A. (1999). Users are not the enemy. Association for Computing Machinery. Communications of the ACM, 42(12), 40 (47 pages)

[2] Anderson, J. R. (1994). Learning and Memory: An Integrated Approach: John Wiley & Sons Inc

[3] B.DawnMedlin, & Cazier, J. A. (2005). An Investigatieve Study: Consumers Password Choices on Journal of Information Privacy & Security, 1(4), 44.

[4] Burnett, M. (2002, March 7, 2002). Ten Windows Password Myths Retrieved April 12, 2005, from http://www.securityfocus.com/infocus/1554

[5] Hewett, T. T. (1999). Cognitive factors in design (tutorial session): Basic phenomena in human memory and problem solving. Paper presented at the Proceeding of the Third Conference on Creativity & Cognition, Loughborough, UK.

[6] Higbee, K. L. (2001). Your Memory: How It Works & How To Improve It (2 ed.). New York, NY: Marlowe & Company.

[7] Ives, B., Walsh, K. R., & Schneider, H. (2004). The Domino Effect of Password Reuse. Association for Computing Machinery. Communications of the ACM, 47(4).

[8] Miller, G. A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. Psychological Review, 63, 81-97.

[9] Newell, A., & Simon, H. A. (1972). Human Problem Solving. Englewood Cliffs, NJ: Prentice-Hall.

[10] Sans.org. (2013). Password Policy: www.sans.org.

[11] Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'Weakest Link' -- a Human/Computer Interaction Approach to Usable and Effective Security. BT Technology Journal, 19(3), 122.

[12] Schneier, B. (2000). Secrets and Lies. New York: John Wiley and Sons.

[13] Warkentin, M., Davis, K., & Bekkering, E. (2004). Introducing the Check-Off Password System (COPS): An Advancement in User Authentication Methods and Information Security. Journal of Organizational and End User Computing, 16(3), 41 (18 pages)

[14] Zviran, M., & Haga, W. J. (1999). Password security: An empirical study. Journal of Management Information Systems, 15(4), 161 (125 pages).

INSTRUCTIONS TO CONTRIBUTORS

Information Security is an important aspect of protecting the information society from a wide variety of threats. The International Journal of Security (IJS) presents publications and research that builds on computer security and cryptography and also reaches out to other branches of the information sciences. Our aim is to provide research and development results of lasting significance in the theory, design, implementation, analysis, and application of secure computer systems.

IJS provides a platform to computer security experts, practitioners, executives, information security managers, academics, security consultants and graduate students to publish original, innovative and time-critical articles and other information describing research and good practices of important technical work in information security, whether theoretical, applicable, or related to implementation. It is also a platform for the sharing of ideas about the meaning and implications of security and privacy, particularly those with important consequences for the technical community. We welcome contributions towards the precise understanding of security policies through modeling, as well as the design and analysis of mechanisms for enforcing them, and the architectural principles of software and hardware system implementing them.

To build its International reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJS.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Starting with Volume 8, 2014, IJS appears in more focused issues. Besides normal publications, IJS intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

We are open to contributions, proposals for any topic as well as for editors and reviewers. We understand that it is through the effort of volunteers that CSC Journals continues to grow and flourish.

IJS LIST OF TOPICS
The realm of International Journal of Security (IJS) extends, but not limited, to the following:

- Anonymity
- Attacks, security mechanisms, and security service
- Authorisation
- Cellular/wireless/mobile/satellite networks securi
- Public key cryptography and key management
- Cryptography and cryptanalysis
- Data integrity issues
- Database security
- Denial of service attacks and countermeasures
- Design or analysis of security protocols
- Distributed and parallel systems security
- Formal security analyses
- Information flow
- Intellectual property protection
- Anonymity and pseudonymity
- Code security, including mobile code security
- Biometrics
- Authentication
- Confidentiality, privacy, integrity, authenticatio
- Data confidentiality issues
- Data recovery
- Denial of service
- Dependability and reliability
- Distributed access control
- Electronic commerce
- Fraudulent usage
- Information hiding and watermarking
- Intrusion detection

- Key management
- Network and Internet security
- Network security performance evaluation
- Peer-to-peer security
- Privacy protection
- Revocation of malicious parties
- Secure location determination
- Secure routing protocols
- Security in ad hoc networks
- Security in communications
- Security in distributed systems
- Security in e-mail
- Security in integrated networks
- Security in internet and WWW
- Security in mobile IP
- Security in peer-to-peer networks
- Security in sensor networks
- Security in wired and wireless integrated networks
- Security in wireless communications
- Security in wireless LANs (IEEE 802.11 WLAN, WiFi,
- Security in wireless PANs (Bluetooth and IEEE 802.
- Security specification techniques
- Tradeoff analysis between performance and security
- Viruses worms and other malicious code
- Multicast security
- Network forensics
- Non-repudiation
- Prevention of traffic analysis
- Computer forensics
- Risk assessment and management
- Secure PHY/MAC/routing protocols
- Security group communications
- Security in cellular networks (2G, 2.5G, 3G, B3G,
- Security in content-delivery networks
- Security in domain name service
- Security in high-speed networks
- Security in integrated wireless networks
- Security in IP networks
- Security in optical systems and networks
- Security in satellite networks
- Security in VoIP
- Security in Wired Networks
- Security in wireless internet
- Security in wireless MANs (IEEE 802.16 and WiMAX)
- Security policies
- Security standards
- Trust establishment
- WLAN and Bluetooth security

CALL FOR PAPERS

Volume: 8 - **Issue:** 2

i. Submission Deadline : April 5, 2014 **ii. Author Notification:** May 5, 2014

iii. Issue Publication: May 2014

CONTACT INFORMATION

Computer Science Journals Sdn BhD

B-5-8 Plaza Mont Kiara, Mont Kiara
50480, Kuala Lumpur, MALAYSIA

Phone: 006 03 6204 5627
Fax: 006 03 6204 5628
Email: cscpress@cscjournals.org

CSC PUBLISHERS © 2014
COMPUTER SCIENCE JOURNALS SDN BHD
B-5-8 PLAZA MONT KIARA
MONT KIARA
50480, KUALA LUMPUR
MALAYSIA

PHONE: 006 03 6204 5627

FAX: 006 03 6204 5628
EMAIL: cscpress@cscjournals.org