International Journal of u- and e- Service, Science and Technology
Vol.8, No. 9 (2015), pp.371-380
http://dx.doi.org/10.14257/ijunesst.2015.8.9.36

Analysis of Password Generation Types in Teenagers –Focusing on the Students of Jeollanam-do

KwangCheol Rim[1] and SoYoung Choi[2]

[1] *Department of mathematics, Chosun University, KwangJu, Korea,*
[2]*Department of mathematics, Chonnam National University, KwangJu, Korea*
rim1201@hanmail.net, Audry5100@korea.com

Abstract

Password generation and password management are the most important factors in information security. Hence, this study measures the degree of inclusion of information that is identical or similar to personal information among the passwords generated by teenagers. It is reported that for each teenager there are approximately 3.3 passwords and the number of passwords that need to be managed by individuals is constantly increasing due to rapid expansion of the Internet of Things. The results of this study showed that, of the student generated passwords, 40% are similar to their IDs and 70% are consistent with their personal information. Out of these, 67.5% of the respondents stated that they did not periodically change their passwords. It also indicated that 87.5% of the passwords consist of both characters and numbers, which are a general characteristics of passwords generated by the people in Korea, and only 1.1% of the passwords include special characters. It was also found that 32.2% of the students experience hacking incidents, of which 53.7% of the incidents occur in games and 34.5% in portal sites; this implies that students become victims of hacking in cyber space that they use frequently. However, information security education in school does not provide detailed information on passwords, thus requiring urgent improvement.

Keywords: *password, Generated Password, password management, Information Security Education*

1. Introduction

Computer users today are not very security conscious while selecting and entering passwords and tend to choose passwords that can be easily guessed. In this regard, security education related to passwords, which are the first targets for hacking, should be provided thoroughly and organizations should establish criteria for selecting and entering passwords [3].

Development of various information technology systems has led to an exponential increase in the number of IDs and passwords required to be generated by users; these are being constantly generated for management of various applications and operating systems. Under these circumstances, efforts for preventing exposure of passwords are being made and the need for education on password generation is being emphasized.

On April 13, 2015, hackers claiming to be members of Sunni Muslim militant groups and Islamic States (IS) threatened an attack similar to that of the 9/11 bombing in the US, releasing a message stating that they would destroy national cyber security systems from within [1].

Similarly, in January 2015, documents containing the names of retired generals and locations of military bases in America were leaked, and President Barack Obama was threatened after the US Central Command's Twitter account was hacked [2].

ISSN: 2005-4246 IJUNESST

According to recent trends as presented by the Cyber Terror Response Center of the Korean National Police Agency, the number of cybercrimes increases each year. Given that teenagers commit nearly 30% of all cybercrimes, it is clear that the internet has an immensely adverse effect on teenagers [3]. Moreover, it was recently reported that approximately 50% of 900 teenagers experience profanity and backbiting on the Internet. Thus, damage due to the indiscreet usage of the Internet by teenagers is increasing. The most common reasons teenagers use profanity and backbiting online are reportedly because of "revenge" (47.9%), followed by "no reason," "fun," and "relief of stress," in decreasing order. In addition, 70% of respondents said that they did not feel guilty after using foul language online. This indicates that teenagers have grown desensitized to slander and profanity [10].

Preventing advanced hacking attacks require both a professional workforce and improved information security awareness; however, these two requirements are not being completely met in Korea. Among the various reasons for workforce issues, the lack of systematic information security education in Korea is considered to be one of the most important one. In South Korea, the Central Official Training Institute of Ministry of Public Administration and Security, and Korea Internet & Security Agency, including several private institutes, provide information security education.

Unlike the US, South Korea has no master plan at the national level for online privacy protection education; furthermore, the privacy protection education currently offered throughout the nation is not producing any sizable results, due to lack of various programs and of information exchange between institutions that offer such programs. Additionally, because most privacy protection education programs target adults, they do not increase privacy protection awareness in elementary, middle, and high school students (or even the general public).

In this study, existing literature on password configurations is reviewed. The use of passwords by middle and high school students is then analyzed through a survey in section 3; the need for in-depth privacy protection education in educational institutions is discussed in the conclusion.

2. Previous Research

2.1. Research Related to the Password

As According to V. Ashlee, the most frequently used password is "12345," followed by "password," "iloveyou," "princess," and "abc123," among others [4]. A study by R. Shay and colleagues showed that 80% of respondents used the same password for many different sites, and that 70% used the same password with only slight variations for different accounts [5]. A study by G. Beate and colleagues showed that people used seven to eight different passwords, and tended to reuse one password in many different places [6]; L. Armstrong found that participants used their own names, nicknames, addresses, and birthdates, or words easily found in dictionaries [7]. A study by L.W. Andrews found that 48% of participants used information related to themselves or their families as passwords, and that less than 10% used difficult passwords that could be deemed indecipherable [8]. A password survey of college students in South Korea also revealed that almost 50% of passwords were related to personal information, and that more than 10% were either easy to remember or easy to type [9].

2.2. Curriculum Related to Information Security in South Korea

Table 1. Curriculum Related to Information Security in South Korea

Category	Subject area	Subject title	Educational details
Elementary school	Common curriculum	Ethics	Public order and Internet etiquette
		Practical Arts	Characteristics of and ethics in cyber space
	Creative activity	Guideline for Information and Communication Technology	-Information security and password -Viruses and spam mail -Encryption and security programs -Copyright
Middle school	National common basic curriculum	Technology and Home Economics	-Information ethics and personal information protection -Intellectual property rights
	Elective curriculum	Information	-Personal information protection -Information exchange and management -Information protection technology and Intellectual property rights
	Creative activity	Guideline for Information and Communication Technology	Encryption and information protection technology
High school	Elective curriculum	Information	Information ethics and information technology
	Creative activity	Guideline for Information and Communication Technology	Law on information protection

Table 1 describes the details of the curriculum related to information security in elementary and middle schools. In elementary schools, information security education is provided initially in the form of creative activities. Then, protection against viruses is taught at the second stage, and computer encryption and security programs are explained at the third stage. In middle schools, content on information security is included in subjects related to technology, and home economics and information; the Guideline for Information and Communication Technology is used in creative activities to provide students with information security education. In high schools, students learn not only about information security technology, but also legal knowledge that is relevant.

As shown in Table 1, information security education in Korea is provided in the form of basic principles of information ethics and information technology. For this reason, students do not have an opportunity to practically learn about personal

information protection, practice information ethics, or participate in relevant practical activities. In addition, the number of competent teachers who can provide students with information security education and educational environments are not sufficient; practical details on personal password management, which is a crucial element for information protection, as well as password generation and storage are not included in the education.

3. Password Survey of Middle and High School Students

A survey was conducted on 1000 middle and high school student in the province of Jeollanam-do; after excluding insincere responses, descriptive statistics were performed on 550 responses. The participants included 307 female students and 243 male students.

Students participated in the survey, with a serious attitude, in the presence of their homeroom teachers and all the data related to the passwords, recorded in the survey, were discarded after the research analysis. Moreover, it was strongly recommended to the students to avoid using passwords recorded in the survey and use new passwords that include special characters and do not include any personal information.

3.1. Number of Passwords in Use and Their Similarity to Private Information

Table 2. The Number of Passwords in Use

Number of different passwords	N	Percentage (%)
1	49	8.9
2	114	20.7
3	147	26.7
4	77	14.0
5 or more	163	29.6

When asked about the "number of different passwords in use," 91.1% responded that they used two or more, with 43.6% (240 respondents) indicating that they used four or more. The number of passwords in use by the respondents may be considered large, as the number of IDs and passwords per person is expected to increase, given the various internet uses employed by middle and high school students.

Table 3. Similarity Between ID and Password

Similar elements	N	Percentage (%)
Letter	125	22.7
Number	67	12.2
Letter + number	17	3.1
Dissimilar	341	62
Total	550	100

When asked about the "similarity between IDs and passwords," 209 respondents (38% of total responses) reported that their IDs and passwords shared certain elements. About 22.7% of all participants—60% of those who reported having IDs and passwords with shared elements—indicated that their IDs and passwords contained the same letters.

Table 4. Similarity between Password and Personal Information

Personal information	N	Percentage (%)	Personal information	N	Percentage (%)
Name	354	64.4	Preferred number	111	20.2
Birthday	229	41.6	Nickname	105	19.1
Cellular phone	228	41.5	Address	80	14.5
Home phone	150	27.3	Family's information	76	13.8
Resident registration number	125	22.7	Friend's information	24	4.4

Redundancy was allowed in the survey for measuring the degree of personal information inclusion in passwords. When asked about the amount of personal information included in passwords, 354 respondents (64.4% of all respondents) indicated that their passwords were identical to their names, and 41.6% and 41.5% indicated that their passwords included birthday and cellular phone information, respectively. As shown in Table 3, students tended to generate passwords by combining personal information, which can be easily recalled. If direct and indirect information such as information related to students' families and acquaintances is also included, then most passwords are said to be generated based on personal information.

Table 5. Number of Components in Consistent IDs and Passwords

Number of consistent parts	N	Percentage(%)	Valid percentage(%)
1	5	0.9	2.4
2	13	2.4	6.2
3	49	8.9	23.4
4	51	9.3	24.4
5	28	5.1	13.4
6	19	3.5	9.1
7	17	3.1	8.1
More then 8	27	5.0	13.0
Total	209	38.2	100

The result of calculating the number of components for consistent IDs and passwords, depending on the students who stated that they had IDs similar to their passwords, showed that the percentage of consistent components being three to five was 61.2. This indicates that more users use three to five components consistently in both their IDs and passwords. It was also found that the number of components shared in both the ID and password is approximately 4.6.

3.2. Password Duration

Table 6. Password Change Frequency

Change frequency	N	Percentage(%)
1 month	16	2.9
3 month	40	7.3
Half a year	48	8.7
1 year	54	9.8
Do not change	371	67.5
Other	21	3.8
Total	550	100

Regarding the question of the time period for changing the password, it was found that merely 10% of the students changed their passwords every three months and 18.5% changed once a year. On the other hand, 371 students (67.5%) stated that they never change their passwords, indicating that most students do not change their passwords once generated.

3.3. Password Configurations

Table 7. Individual Password Configurations

Assortment	N	Percentage (%)
Only number	14	2.5
Only letter	18	3.3
number + letter	37	6.7
letter + number	481	87.5
Total	550	100

Six passwords included special letters, accounting for 1.1% of all the passwords; 5.8% passwords consisted of only numbers or letters. On the other hand, 94.2% passwords had a combination of numbers and letters and 87.5% included letters at the beginning and numbers at the end. This result confirmed that most students use passwords that have a combination of letters and numbers, which can be easily predicted.

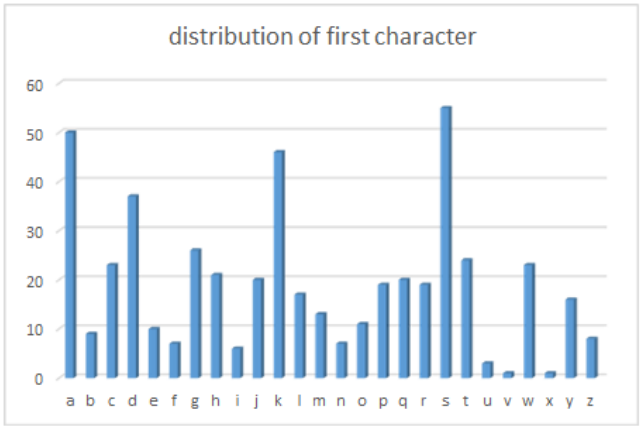

Figure 1. Password First Character Frequency

To analyze a possibility of distinguishing characters used in passwords, the frequency of characters selected as the first character of the password was examined. As for the first letters, ‘a’, ‘s’, and ‘d’, which are placed on the home row on a QWERTY Keyboard, were used most frequently, accounting for 10.2%, 11.2%, and 7.5%, respectively, of all the passwords; the frequently used letter “k” in Korean last names, was used 46 times, accounting for 9.3% of all the passwords. The result shows that the frequency of the first character was consistent with that of general alphabets, thereby confirming that students used characters and personal information that can be easily used.

3.4. Experience of Hacking Damage

Table 8. Hacking Damage

Damage	N	Percentage(%)	Valid percentage(%)
Once	111	20.2	62.7
Twice	30	5.5	16.9
More then 3	36	6.5	20.4
None	373	67.8	
Total	550	100	100

Among the respondents, 32.2% experienced hacking incidents. As for the hacking incidents, 111 students stated that their accounts were hacked once; in addition, 66 accounts were hacked twice, accounting for 37.3% of all the victims of hacking. The victims changed their passwords after being hacked, but still included personal information in their passwords.

Table 9. Hacking Channels

Assortment	N	Percentage (%)	Valid percentage (%)
Portal site	61	11.1	34.5
Game	95	17.3	53.7
SNS	21	3.8	11.7
Total	209	32.2	100

Regarding the channels of hacking incidents, game websites accounted for 53.7%, which is the highest ratio, followed by portal sites. That is because young students use games and portal sites more frequently than SNS and emails. Moreover, it seems that such hacking incidents were caused mainly by shoulder attacks due to Trojan viruses or the PC room culture, which is highly developed in Korea, rather than professional hacker groups.

4. Conclusion

The personal information of approximately 83 million people was leaked from JP Morgan Chase & Co. just a year ago (Nov. 2014), while Sony Entertainment suffered damages of up to one hundred million dollars from the leakage of unreleased movies (Nov. 2014). Similarly, personal information of over 80 million people was leaked from Anthem, a health insurance company, in February 2015. The personnel management departments of government organizations in the United States reported that although this result is based on selective data, 21.5 million employees were affected by data loss due to attacks by cyber criminals and the personal information of 22 million employees was leaked among all the employees

affected by hacking. This figure accounts for approximately 7% of the entire American population, which is a considerable amount [11].

Based on these incidents, it may be surmised that an enormous quantity of personal information has been leaked thus far. The fact that the passwords of middle and high school students depend on personal information—and that almost 70% of students do not change their passwords—proves that privacy protection education in schools is ineffective

Students are likely to generate typical passwords based on the culture of the society to which they belong, without being provided education regarding professional information security. Moreover, they generate passwords by combining information that is exposed excessively such as names, birthdays, and resident registration numbers, and neglect their passwords once they are generated.

As shown in the present study, vigilance for protection of passwords and personal information among middle and high school students is practically non-existent; an education plan capable of addressing this problem is urgently needed.

References

[1] "ISIS Threaten America with Another 9/11", Newsweek, **(2014)** April 13.
[2] "The Newsweek Twitter Account Was Hacked By ISIS Supporters", Buzz Feed NEWS, **(2015)**.
[3] C. Raphael and W. Phan, "Cryptanalysis of two password-based authentication schemes using smart cards", Computer and Security, vol. 25, **(2006)**.
[4] V. Ashlee, "Most Common iPhone If Your Password Is 123456", Just Make It Hack Me, The New York Times, **(2010)**, Http://amitay.us/blog/files/most_common_iphone_passcodes.php.
[5] R. Shay, S. Komanduri, P. G. Kelley, L. Bauer, P. G. Leon, N. Christin, M. L. Mazur and L. F. Cranor, Encountering Stronger Password Requirements: User Attitudes and Behaviors, Symposium on Usable Privary and Security(SOUPS), **(2014)** July 14-16 Remond, WA, USA.
[6] G. Beate and J. Hilary, "Using and Managing Multiple Passwords", Ligehacker, **(2010)**, Http://www.lifehacker.com.au/2010/03/how-id-hack-your-weak-passwords/.
[7] L. Armstrong, "And the Passwords is", Business Week, vol. 3785, no. 89, **(2002)**.
[8] L. W. Andrews, "Passwords Reveal Your Personality", Psychology Today, vol. 35, no. 16, **(2002)**.
[9] S. K. Moon, "A study on the using pattern analysis of four-digit personal identification numbers – A university case", Journal of Digital Convergence, vol. 10, no. 10, **(2012)**.
[10] J. M. Ryy, K. M. Kim, S. H. Cho and S. S. Kim, "The Instructional Design of Information Communication Ethics Based on Integrated Character of Lickona", Journal of Korea Association of Information Education, vol. 14, no. 3, **(2010)**.
[11] http://www.computing.co.uk/ctg/news/2412920/hackers-have-stolen-personal-data-on-every-us-federal-employee-claims-union.
[12] Y. J. Jang, D. H. Kim, H. S. Kim, W. G. Lee and H. C. Kim, "Development of Unplugged Activity and its Evaluation of Usability for Information Security Education", Journal of Korea Association Computer Education, vol. 14, no. 1, **(2011)**.
[13] K. C. Rim, "Advanced Science and Technology Letters ASTL103", Investigation and Analysis of Password Use for the Betterment of Privacy Protection Education in Middle and High School Students, **(2015)** August 19-22, Jeju island, Korea.

Authors

KwangCheol Rim, received the PhD. Degrees in Mathematics from Chosun University in 2006. He is currently a researcher in Information Technologies and information security. His current research interests are quantum cryptography, endpoint security and information education.

SoYoung Choi, received the PhD, Degrees in mathematics from Chonnam National University in 2003. She is currently a researcher in Information Technologies and information security and Rim's assistants.