computing@computingonline.net
www.computingonline.net

ISSN 1727-6209
International Journal of Computing

PASSWORD PROTECTION: END USER SECURITY BEHAVIOR

Keisuke Kato [1], Vitaly Klyuev [2]

[1] Department of Computer Science and Engineering, University of Aizu, Fukushima, Japan, s1190085@u-aizu.ac.jp
[2] Department of Computer Science and Engineering, University of Aizu, Fukushima, Japanvkluev@u-aizu.ac.jp, http://www.u-aizu.ac.jp/~vkluev/

Abstract: Password authentication is one of essential services in our life for protecting data. In other words, we may loose a lot of money, sensitive data, etc., if passwords leak out. Thus, we have to understand clearly what is important for creating and/or changing passwords. Our goal is to analyze key issues for setting passwords. We surveyed 262 students of the University of Aizu, Japan. We discussed key security problems, main password protection issues and techniques, and misunderstandings about passwords by end users. Furthermore, we compared the obtained data with results provided by the National Institute of Standard Technology (NIST) and others. The results can help the users set stronger passwords.

Keywords: Security, Password Protection, User Study, Survey, Tendency.

1. INTRODUCTION

In the last decade, a growing number of Internet services made password authentication very important to protect our sensitive data. On the other hand, cracking attacks to steal user passwords increased rapidly. To make password protection stronger, techniques such as two-step verification [1] and two-factor authentication [2] were developed. However, a password is not the only way to authenticate users in the systems.

Book [3] discusses three key options for authentication. The first one is to retain physical control on the device such as a remote car door key. The second one is to use a password. The third option is to utilize something like a fingerprint or iris pattern. However, for the cost reason, most systems work only with passwords. Thus, we need to understand all possible details about passwords. To obtain good knowledge on password authentication, there are a lot of sources. To understand password security better, we consider the problem from three different directions:

- Will the user be able to remember the password?
- Will the user choose a password that is hard to crack or guess?
- Will the user reuse the password on other systems and/or applications?

In this paper, we seek better understanding of the tendencies that create and/or change passwords. We discuss key security problems, tendencies in password protection techniques, misunderstandings by the users, etc. We present the results of a survey of 262 University of Aizu undergraduate students. Based on the analysis of literature, we suggest some practical recommendations to set a strong password as a framework for our investigation. The suggestions and results of our investigations are useful for the end user to help in setting it.

This paper is based on study [4]. It is organized as follows. In Section 2, we briefly review the recent publications examining password protection issues. In Section 3, we propose a framework to set strong passwords. In section 4, we give detailed information about the survey and discuss basic issues to analyze user data. In Section 5, we analyze the tendencies in password protection, examine the results of the survey, and compare them with data from other sources. In Section 6, we highlight our significant findings.

2. RELATED WORK

For a cracker, the first step to crack a password is to encrypt the possible password candidates and to compare the result values with the values of the encrypted real password. There may be vulnerability in a system or crackers can find the vulnerability faster than specialists in security can do that. So, crackers may attack the vulnerability utilizing several ways. The one of the common ways to break the passwords is to scan the whole space of the character set used in passwords for a brute force attack. The one-way functions or algorithms such as

MD5, SHA etc. are very fast to run. For crackers, however, this is very important because they can use a brute force attack easily. Based on this, a time-effective approach is to think about the candidates that are to be the actual words, patterns, or combination of the characters, which are not difficult to remember [5].

Another common way used in practice is a dictionary attack. In the past, some systems that use an encrypted password file made it readable. Users may fetch this file and then try to break passwords offline by using a dictionary. Thus, a cracker encrypts the values in his dictionary and compares them with the records in the file. This activity is called a dictionary attack. Actually modern operating systems have fixed this problem. However, the dictionary attacks are still implemented. Study [6] discusses fast dictionary attack algorithms by using time-space tradeoff and actually their algorithm recovered 67.6 % of the passwords using a 2×10^9 search space.

There are several cracking tools available to crack or guess passwords. Two objects are the targets of cracking tools: passwords and the function for administrators to reactively check the passwords used in the system. The reactive checking may increase the system security by finding the easy to crack passwords and by warning the related uses to change their passwords to protect their accounts from being cracked by intruders [5]. *John the Ripper* and *Hashcat* [7, 8] are the tools to analyze and provide information on methods used by crackers.

Report [26] shows the statistical data on privacy issues. They are compared with results of investigations [27] by The Institute for Prospective Technology Studies (IPTS) that is one of seven scientific institute of the European Commission's Joint Research Centre. Data in Table 1 and 2 are excerpts from the aforementioned report.

Table 1 illustrates the different view of Japanese and EU citizens on the privacy issues. Data from Table 2 give answers to the question about the responsibility for leaking the private data on the Internet. Japanese users want another person or company to take responsibility. A view of EU users is different: the user itself should take it. Thus, Japanese users have different understanding of security issues compared to people from other countries.

Table 1. Positive answers to the question: Could you provide your private data online?

Data type	IPTS	Japanese user
Name	86 %	37 %
Address	65 %	19 %
Own Photo	58 %	7 %
Bank Information	30 %	4 %

Table 2. Who should take a responsibility for leaking private data?

Answer	IPTS	Japan
The user should take a responsibility	32 %	38 %
The company that has the private data should take a responsibility	27 %	40 %

3. PRACTICAL SUGGESTIONS

Analysis of literature on security issues and users misunderstandings [11, 16–19] allows us to state the following conclusions:

- A long password is not always equal to the strong password. When someone sets the passwords, s/he should avoid usage of a language grammatical structure, which helps memorize passwords [11].
- A password consisting only of numerical characters or only alphabetical characters such as only upper-case or only lower-case is very dangerous. It will be easily cracked or guessed. The users should use numerical and alphabetical characters to set passwords [17, 19].
- To be hard to guess or crack password, the user should use many types of characters as possible. Because the password strength would be stronger if the password's entropy was bigger.
- In order to memorize passwords, it recommend that users use a password management tools such as *LastPath, 1Password, KeePass, Password Dragon*, etc. [18]
- To use a password management tools, you can reduce a burden of creating and changing password. Because the tools can generate random password automatically and the user should memorize only master password.
- Users should avoid the use of passwords such as *"password"*, *"abc123"* and personal data such as name, birthday, address, telephone number, etc. directly. Unfortunately many users set such passwords and crackers are familiar these oversights.
- A password that is usable as an abbreviation from a phrase of sentence is useful for end users to memorize.
- The user should not tell any person their passwords and should not share it with any person.

These suggestions, we consider as a framework for investigations.

Taking into account the differences in user behavior mentioned in Section 2, we analyze these issues considering the students of University of Aizu.

4. QUESTIONNAIRE

In this study, the main method to detect key details in creation and changing passwords is to survey the students of University of Aizu who use the Internet in everyday life. We start with an overview of the questionnaire used in this study. A survey on password protection issues was conducted in April 2013 at the University of Aizu. The participations are 163 2nd year undergraduate students and 99 3rd year undergraduate students majoring in Computer Science. Every participant is a native Japanese and age is between nineteen and twenty-two years old. The questionnaire is in Japanese, the mother language of participants. The questionnaire in the paper-based format was distributed among students. It consists of 15 questions. A goal of this survey was to get the information on password usage by users who are unprofessional in security.

Table 3. Classification of questions in questionnaire.

Elements of a password	Q1. How many characters does your password have? Q10. How many lower-case letters are in your current password? Q11. How many upper-case letters are in your current password? Q12. How many digits are in your current password? Q14. How many different passwords do you have?
Strategy of a password setting	Q2. When you create new or change your password, do you write down it on the paper? Q3. Do you use the same password for different accounts? Q5. Which strategy is more applicable to select your passwords? Q6. Do your passwords have some components such as your name or birthday?
Recognition of a strong password	Q8. How often do you change your password on accounts except the university account? Q13. Do you think your password is strong? Q15. Which of following three passwords is stronger password?

We have to get evidence on reliability of our data. To do that, we focus on two things that are the number of questions in the questionnaire and the rate of respondents who did not answer the questions. In questionnaire, every participant can choose *"I prefer not to answer"* for each question except for the last one. Study [9] analyzed 100,000 respondents and found that if a respondent begins answering a survey, the sharpest increase in drop-off rate occurs with each additional question up to fifteen questions and if the respondent is willing to answer fifteen questions, the drop-off rates for each incremental question, up to thirty-five questions, is lower than for the first fifteen questions added to a survey. And the respondent drop-off rate that consists of fifteen questions is between 4 % and 6 %. In our survey, we counted the rate of respondents who chose *"I prefer not to answer"* and/or did not answer more than twelve questions (80 % of the total number of questionnaire questions). 4 % (11 students out of 262 students) answered in such a way. It means our data are similar to the Survey Monkey's survey [9]. Thus, our data are reliable.

The questionnaire covers a wide range of problems in password security. The questions can be separated into three main groups: "Elements of a password", "Strategy of setting a password" and "Recognition of a strong password" (See Table 3).

In the group of *Elements of a Password*, we asked about elements of user passwords such as password length, type of characters in the password, etc. In the group of *Strategy of Setting a Password*, we tried to understand what strategies of creating and/or changing passwords are utilized by users. However, we could not find a strategy and predict it from this questionnaire. However, in the group of *Recognition of a Strong Password*, we tried to uncover the user's understanding of the strong password and we got one issue from these answers about it.

5. MAIN PASSWORD PROTECTION ISSUES

We hope that end users can set strong passwords in the future. However, now the Internet community is facing many problems. One of the most prevalent misunderstandings is a security issue. In this section, we focus on this problem. We discuss which information is true and which is not.

We illustrate the results of discussions by using survey data and data from others sources [5, 10–13, 20–24].

5.1. DIFFICULTIES WITH A PASSWORD STRUCTURE

As we mentioned in Section 3, there are some recommendations about password structure because it is very important and this is one of point that a lot of end users misunderstand and feel difficulty.

The results of our survey show that 8 % of respondents (22 students) said that their passwords are strong and 16 % of respondents (42 students) said that their passwords are weak. Fig. 1 shows the results that separate groups based on student's opinion about their own password. The mean of password length for a strong group is 10.1, for a weak group is 8.3 and for a normal group is 9.1. Thus, their opinion about password strength is objective.

Another interesting outcome is as follows: 43 % (114) of students use the same password for different accounts such as Google account, Facebook account, etc. The average number of accounts used with the same password is 5.4. Study [22] found that the ordinary user has 25 password-protected accounts on average. So, most participants of the survey use the same password for different accounts. Study [13] shows that about 30 % of users use the same password four or more times. Thus, we need a strategy to set a strong password by every end user.

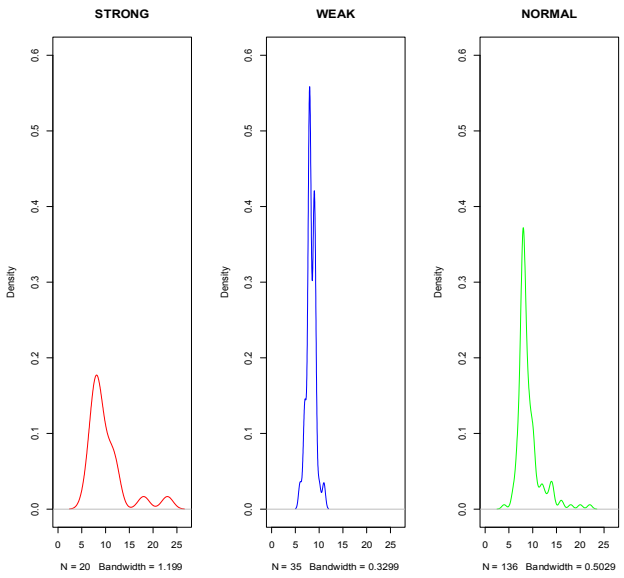

Fig. 1 – Password strength and password length.

We tried to understand strategies to set new passwords from the data of our survey but we could not detect any common patterns. We analyzed the following selections for this issue.

- Password based on the first letter of each word in a phrase.
- Password based on a phone number.
- Password based on an address.
- Password based on a birthday.
- Password based on a word or name with numbers or symbols added to the beginning or end of the term. (A symbol is a character which does not belong to the letters on digits)
- Password based on a word or name with numbers and symbols substituting some of the letters.
- Password based on a word in a language other than English.
- Abbreviation consisting of the first characters of the phrase/sentence.
- Others

36 % (96) of students selected "Others" and 16 % of students selected *"I prefer not to answer"*.

The length of the passwords is very important issue in the password protection. From our observation, we found that many users have one big misunderstanding related to this parameter. It is about long passwords. Actually, many users believe that long passwords are equal to strong passwords but this is not true. Why the long password is not equal to the strong password? All users must memorize the long passwords. However it is very difficult for them to memorize the string like this "qVwN2s6K@Ka". Thus, they create the long password that is very easy to memorize and then many users use a grammatical structure such as "Ihave3cats" for the passwords [11]. This password may be long but applying the dictionary attack, it can be easily guessed. As a result, the possibility to crack or guess increases from 6 % to 20.5 % [11].

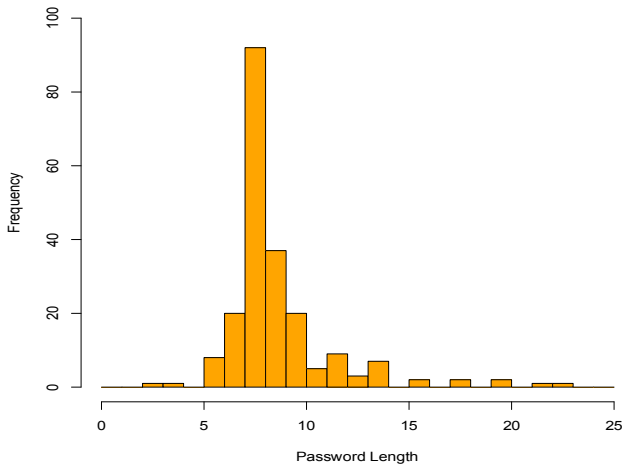

Fig. 2 – Password length.

We carefully analyzed resulting sheets. Fig. 2 shows the password length distribution. The mean of password length is 9.1 characters. Fig. 3 and Table 4 show the difference in distribution between second year and third year students. For the 2nd year students, the standard deviation is 2.4 but for the third year students, the standard deviation is 3.0. Fig. 4 shows the difference in density in password length between the 2nd year and 3rd year students. The graph of the density for the 3rdyear students is shaper compared to that for 2ndyear students. It means that third year students have more variations in password length compared to the second year students.

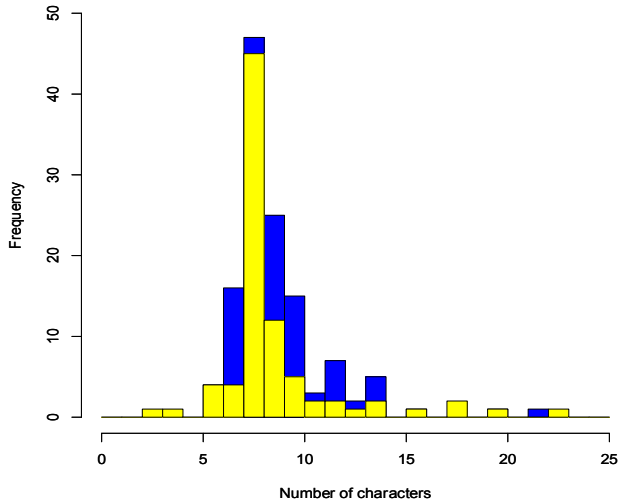

Fig. 3 – Difference between 2nd year and 3rd year students.

Table 4. Difference in standard deviation (SD) between 2nd year and 3rd year students.

Question Summary	σ (2nd year)	σ (3rd year)
Password Length	2.409025	3.071228
Number of lower-case letters?	2.832335	3.421342
Number of upper-case letters?	1.646054	2.66999
Number of numerical letters?	1.667903	3.61654

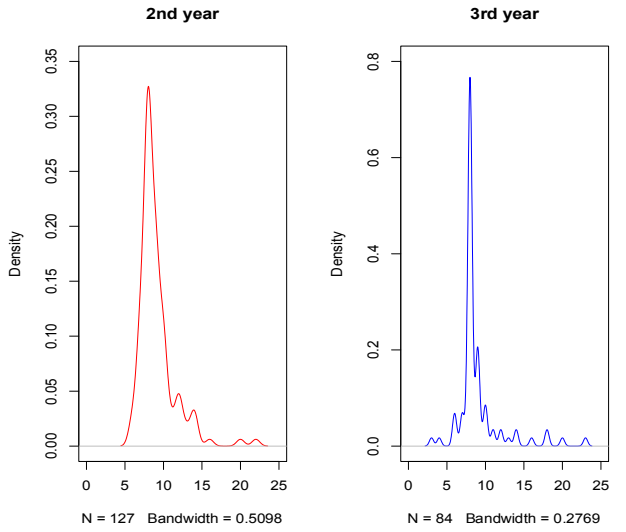

Fig. 4 – Density of password length.

Study [5] shows the relationship between the password length and strength of passwords. The portion of the strong passwords (passwords which were not cracked) with the length of 7 characters has a proportion of 96 % among the whole passwords. Such a high percentage is not observed for the passwords with the length less than 7. According to these results, number 7 is the critical threshold value of the password length and the passwords including less than 7 characters may be considered as weak passwords. Another data related to the character length of the passwords is that the passwords with the exact length of 8 characters have a rate of 45 % among the all passwords. This last observation implies that the users have a high tendency to choose passwords consisting of 8 characters.

Study [11] suggests not to use Part-of-Speech tagging system strategies such as "Determiner Adjective Noun" to set a password because it is easy to crack passwords by utilizing common cracking approaches characterized in Section 2.

5.2. DIFFICULTIES WITH MEMORIZING PASSWORDS

The password problem may be summed up as *"Choose a password that is difficult to remember and don't write down it on paper"* [3]. Book [3] discusses problems related to memorizing passwords under four main headings.

1) Naive Password Choice: One possible explanation is that many people try to use the same password everywhere.

2) User Abilities and Training: The best compromise will often be a password checking program that rejects clearly bad user choices, plus a training program to get your compliant users to choose mnemonic passwords. Password checking can be done using a program such as *crack to filter user choices* [14].

3) Design Errors: There are many sources in the Internet to check whether the password is weak or strong. One of them is a password meter [25]. Study [21] found the impact of password meters. At the registration at the online services, the suggestion from password meters is too late. However, at creating a new password, it might have affects.

4) Operational Failures: The user is not only one who is wrong with password selections. Nowadays, there are many web applications utilizing databases that use well-known default master passwords and websites listing the defaults for everything in sight. These passwords will be cracked soon because the default password use well-known patterns and crackers know this fact.

5.3. DIFFICULTIES TO CREATE AND CHANGE PASSWORDS

In this section, we show details about the nature of characters in the passwords. According to the results of our survey, the mean of lower-case characters in the password is 5.1 characters, the upper-case characters is 1.3 characters and the numerical characters is 2.8 characters. These data are similar to data discussed in [10, 12]. Thus, these data are not unique for our university. The main

result is as follows. About 50 % of characters in the passwords are in lower-case.

Study [5] reveals another issue in passwords creation. The users also prefer to include upper-case characters in the passwords. One important issue from these data is that passwords containing at least one punctuation character such as ",!, &, <, >,etc are not used often but the probability to crack them is very low. The outcome from this is: Users may use more often punctuation characters to set strong passwords. From our survey, we observe that 6 % of students use these characters in the passwords.

Fig. 5 illustrates the situation with changing passwords. It shows the distribution of data obtained over periods of time. The value of 0 means that the participant of the survey does not change the password at all. Numbers on the horizontal axis mean the periods in days to change the password. This result is very surprising because about 43 % (115) of students have never changed the password at the resources such as Gmail, Facebook, etc. since they set the password for the first time. Actually, at our university, every student must change the university account password within 90 days since the password has been set. Only 17 % (28) of the second year students have changed the password within this period of time on external services. However we are not planning to force students to change their password because according to [15] changing passwords may improve security but on the other hand, it may increase everyone's frustration. We should note that crackers might be waiting for the change of the password to crack it. Thus, changing the password should be considered very careful.

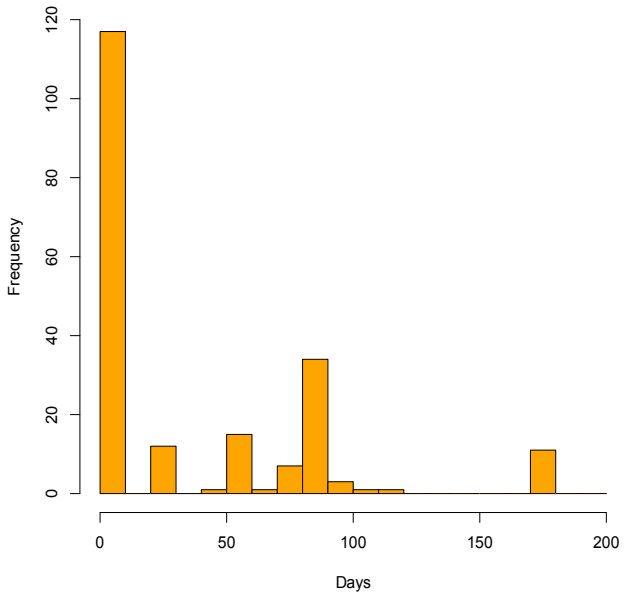

Fig. 5 - Period of time to change the password.

Table 5 shows the rate of participants answering questions touching their privacy. The privacy issue is very sensitive for the mentality of the students answering the survey. Every question in the questionnaire has the selection *"I prefer not to answer"* for participants who don't want to answer the question.

We found an important outcome from our observation: The percentage of the students answered the questions related to privacy (questions from the third column of Table 5) is high and the percentage of the students answered questions not related to privacy (Table 6) is low.

Nowadays, there are very useful tools for end user to create, change, memorize, and manage passwords, called password management tools mentioned in Section 3. Actually some companies and specialists in security have utilized these tools to manage their passwords. And end users who are not specialist in security can also utilize it easily.

Table 5. Answers to the private questions.

Questions	**Students who answered**	**Students who preferred not to answer**
What is the length of your password?	80 % (211 students)	19 % (50 students)
Which strategy is more applicable to set passwords	88 % (168 students)	10 % (26 students)
How often do you change your password?	79 % (208 students)	18 % (48 students)
How many lower-case letters does your password contain?	62 % (163 students)	31 % (83 students)
How many upper-case letters does your password contain?	63 % (165 students)	30 % (81 students)
How many numerical letters does your password contain?	62 % (163 students)	31 % (82 students)

Table 6. Participants selected the option *"I prefer not to answer".*

Questions	**Percent Answering**
Do you think your password is strong?	5 % (13 students)
Do you write down password?	7 % (19 students)
Do you use the same password for different accounts?	8 % (22 students)
Which strategy is more applicable to set passwords	10 % (26 students)
Do you use any strategy to create password?	16 % (44 students)
How often do you change your password?	18 % (48 students)

5.4. PASSWORD STRENGTH

In password security, Shannon entropy [23] is a measure of difficulty guessing a password. A password with a large value of entropy requires a larger number of attempts to guess it, making entropy useful as a measure of password strength [24]. To estimate the amount of entropy in passwords of different length, we need a number of characters, the value of each character and the total value of entropy. However, we do not have these data. We use the NIST guidelines [20]. According to it, these are 2 bits per letter for the entropy. To estimate entropy more accurately, we selected the students who answered the questions that are important for elements of passwords. Here are these questions.

- Q1: How many characters does your password have?
- Q10: How many lower-case letters are in your current password?
- Q11: How many upper-case letters are in your current password?
- Q12: How many numerical characters are in your current password?

Table 7. Mean and standard deviation to estimate entropy.

	Mean	SD
Upper-case	1.328671	2.14534
Lower-case	5.125874	3.153061
Numbers	2.916084	2.704968

We ignored the students who use symbol (punctuation) characters in passwords because we do not know what symbol was used. Only 6 % of users use symbols. The remaining number of student is 143. Table 7 shows the data used for estimating entropy. Our estimated entropy is 27.0 bits. In comparison with results of study [10], the mean of password length is 9.1 and 10.5. However, the entropy is 27.00 bits and 31.01 bits. We see the following reasons for this. There are different trends for password elements. The students of University of Aizu do not use the symbol character; whereas, Carnegie Mellon University students participating in study [10] use many types of character in passwords. The value of entropy for passwords in our study is relatively lower compared to the results of study [10]. According to the NIST guidelines [20], 27 bits entropy are in the passwords consisting of a sequence of 7 characters. Users chose these sequences using dictionaries and composition rules. In our study, the mean of password length is 9.2 for 143 aforementioned students. On the other hand, our entropy fits the sequences consisting of 7 characters. The reason for that is as follows. Our participants do not use symbol characters. Thus, we found that even if a password is long, it does not mean that it is strong because the password strength depends on password length and types of characters.

Comparing our finding with [10, 20], we may conclude that password length is similar in all studies but the value of entropy is very different because the students of University of Aizu do not use symbol characters in pass→words.

5.5. PASSWORD RECOGNITION

The final question in the questionnaire is on the participant understanding of strong passwords. We asked students to select the strongest password among the following:

a) the password that consists of some English phrases or words and it is as long as possible. (ex: thisisstrongpassword)
b) the password that includes numerical, upper-case, lower-case and special characters and it is short. (less than 8 characters)
c) the password that is created as an abbreviation from a phrase of the sentence. (ex : I want to be a great Software Engineer → IwtbgaSE)

26 students selected variant *a*, 182 students selected variant *b* and 35 students selected variant *c*. In Section 5.1, we revealed that the long password is not always a strong password and variant *a* is one such example. It can be easily guessed using grammar tools. Variant *c* is well known way for setting passwords and this is easy for the end user to memorize. However, crackers also know this way for setting and actually they work on how to break passwords created in this manner. So, variant *c* is not weak but not very strong. Variant *b* is actually a strong password. However, for memorizing the passwords, variant *b* is not good for end users.

From this survey, we studied that the end users can distinguish strong passwords. On the other hand, they do not have good strategies to set a strong password by themselves. Actually, in data collected from second year students, 9 % of students selected variant *a*, 71 % of students selected variant *b*, and 10 % of students selected variant *c*. Among the third year students, 11 % of students selected variant *a*, 65 % of students selected variant *b*, 18 % of students selected variant *c*. Thus, understanding the strong passwords is at the same level for second and third year students.

6. CONCLUSION

This study investigates the practical issues related to setting a strong password to use computers, online applications and services. We proposed the framework for practical suggestions to set a strong

password and the questionnaire within this framework. We discussed security issues related to password protection difficulties, misunderstandings in the password protection, difficulties to memorize the passwords, and strategies to change passwords.

Our analysis is based on the survey of 262 University of Aizu students and obtained results are compared with data from different sources. We analyzed key problems for setting a strong password based on separated question groups.

We found that the students of University of Aizu majoring in Computer Science do not pay attention to the practical issues on password protection. They are quite realistic when evaluating the strength of their own passwords. They behave similar to the users from other countries when selecting the length of the password and the password structure. They behave differently when choosing types of character for passwords and passwords strength. They do not clearly understand that the strong password is. This is a one of the reasons why they do not accept the demand to change the password on the regular basis while using Internet services outside the university. 3rd year students are more experienced in computer and Internet applications. They have more variations in password length compared to the 2nd year students.

To improve the situation in password protection, our results from the survey and practical recommendations can help the user set a stronger password.

How to create a strong password? The answer to this question is still an open problem.

7. REFERENCES

[1] Google 2-step verification, http://www.google.com/landing/2step/

[2] Introducing Login Approvals on Facebook, https://www.facebook.com/note.php?note_id=10150172618258920

[3] R. Anderson, *Security Engineering: A Guide to Building Depend- able Distributed System, Second Edition*, Wiley Publishing, 2008.

[4] Keisuke Kato, Vitaly Klyuev, Strong passwords: practical issues, *Proceedings of the 7th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2013),* Berlin, Germany (September 12-14, 2013), pp. 608-613.

[5] I. Korkmaz and M. E. Dalkilic, The weak and the strong password preferences: a case study on Turkish users, *Proceedings of the 3rd International Conference on Security of Information and Networks SIN'10*, pp. 56-61, 2010.

[6] A. Narayanan and V. Shmatikov, Fast dictionary attacks on password using time-space tradeoff, *Proceedings of the 12th ACM Conference on Computer and Communications Security CCS'05*, 2005, pp. 364–372.

[7] John the ripper, http://www.openwall.com/john/

[8] Hashcat, http://hashcat.net/oclhashcat-plus/

[9] Does adding one more question impact survey completion rate? https://www.surveymonkey.com/blog/en/blog/2010/12/08/survey_questions_and_completion_rates

[10] R. Shay, P. G. Kelley, S. Komanduri, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor, Encountering stronger password requirements: user attitudes and behaviors, *Proceedings of the 6th Symposium on Usable Privacy and Security*, 2010.

[11] Ashwini Rao, Birendra Jha, and Gananand Kini, Effect of grammar on security of long passwords", *Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy CODASPY'13*, 2013, pp. 317–324.

[12] M. Dell'Amico, P. Michiardi, and Yves Roudier, Password Strength: An Empirical Analysis, *Proceedings of the IEEE International Conference on Computer Communications*, 2010, pp. 1–9.

[13] D. Hart, Attitudes and practices of students towards password security, *Journal of Computing Sciences in Colleges*, (23) 5 (2008), pp. 169–174.

[14] F. Bergadano, B. Crispo and G. Ruffo, Proactive password checking with decision trees, *Proceedings of the 4th ACM Conference on Computer and Communications Security*, 1997, pp. 67–77.

[15] P. Y. Logan and A. Clarkson, So long, and no thanks for the externalities: the rational rejection of security advice by users", *Proceedings of the New Security Paradigms Workshop NSPW'09*, 2009, pp. 133–144.

[16] C. Herley, Teaching students to hack: curriculum issues in information security, *Proceedings of the 36th Technical Symposium on Computer Science Education SIGCSE'05*, 2005, pp. 157–161.

[17] The maximum time required to analyze password by characters and/or the number of characters in use, http://www.ipa.go.jp/security/english/virus/press/200809/E PR200809.html/

[18] How I'd hack your weak passwords, http://lifehacker.com/5505400/how-id-hack-your-weak-passwords

[19] Password recovery speeds, http://www.lockdown.co.uk/?pg=combi&s=articles

[20] W. E. Burr, D. F. Dodson, and W. T. Polk. *Electronic Authentication Guideline*, Technical report, National Institute of Standards and Technology, 2006.
[21] Serge Egelman, Andreas Sotirakopoulos, Ildar Muslukhov, Konstantin Beznosov, and Cormac Herley, Does my password go up to eleven? The impact of password meters on password selection, *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems CHI'13*, pp. 2379-2388.
[22] D. Florencio, and C. Herley. A large-scale study of web password habits, *Proceedings of the 16th International Conference on the World Wide Web,* ACM Press (New York, NY, USA, 2007), 657–666.
[23] C. E. Shannon, A mathematical theory of communication, *ACM SIGMOBILE Mobile Computing and Communications Review*, (5) 1 (1948).
[24] J. L. Massey, Guessing and entropy, *Proceedings of the IEEE International Symposium on Information Theory*, 1994, 204.
[25] http://www.passwordmeter.com
[26] Recognition and acceptance of security and privacy for eID, Technical Report: (The original title is in Japanese, Copyright © IPA, Japan), http://www.ipa.go.jp/security/economics/report/eid201008.html
[27] Young people and emerging digital services an exploratory survey on motivations, perceptions and acceptance of risks, http://ftp.jrc.es/EURdoc/JRC50089.pdf

Keisuke Kato *is a Bachelor student in the Department of Computer Science and Engineering at the University of Aizu, Japan. His areas of research interest are security Information and Big Data analysis.*

Vitaly Klyuev *received a Ph.D. degree in Physics and Mathematics from St. Petersburg State University (Russia) in 1983. He is presently a senior associate professor at the University of Aizu, Japan. His research domain includes information retrieval, software engineering and analysis of computer algorithms. He has more than 80 publications in referred journals and conference proceedings, three co-authored and eight co-edited books. Dr. Klyuev is a member of editorial board of several academic journals and a program committee member of more than 20 conferences sponsored by ACM, FTRA, IEEE, ISCA, IARIA, and WSEAS.*