Password Education Based on Guidelines Tailored to Different Password Categories

Kirsi Helkala
Norwegian Information Security Laboratory, NISlab,
Gjøvik University College, Norway,
Email: {firstname.surname}@hig.no

Abstract— **General password policies do not guarantee that passwords fulfilling the requirement are good enough. The policies have a tendency to be too broad to be useful for all users. Different users have different designing processes based on what kind of passwords they most easily remember. Users are also often left to generate passwords on their own without any training. In our study we used new password creation guidelines when teaching students password security. We divided passwords into three password categories: Word password, Mixture password and Non-word password. For each category different password generation guidelines were taught to students. Students had access to the password quality measurement tool, which not only measured the strength of the password but also guided students in the generation process. Our goal is to measure the effect of education on the strength of a password and analyze recall rates of the passwords created by the new guidelines. It is shown that education had a positive effect and that passwords became stronger right after the education. The most important result is that a password structure got changed as the variation of structures increased and different structure types were more evenly distributed. However, after half a year without reminders or education repetition, most of the positive effect was lost. While password structures still differed, they had become less complex as participants had given up using special characters. Recall rates of the passwords generated with new guidelines are good.**

Index Terms— **Password security, education, personnel authentication**

I. Introduction

Passwords have existed a long time and are commonly in use. Therefore it is common to think that everybody knows how to create, store and manage passwords without education. However, research shows that this is not the case [7], [11], [13].

When a person generates a password, there is often an easily guessable structure behind. One of the most common password structure is a dictionary word ending with couple of digits [1], [14]. Password cracker tools such as "John the Ripper" start guessing by using pure dictionary words or digits in rising order [15]. In order to avoid this problem, password policies [3], [8], [10] are defined to guide people to generate strong passwords. However, even if a system uses password policy, stating which character sets to use and what the minimum length of a password is, passwords might end up being predictable. Often characters are used in exactly the same order as given in the instructions, and most of the passwords are only as long as the minimum password length. Based on predictable password structures, an adversary can carry out targeted attacks against the system with a greater probability of success.

From the user perspective the general instructions are often too broad to be useful. One remembers best meaningful passwords, some like numbers and special characters while others recall best patterns from the keyboard, etc. The general instructions such as "Minimum length of 8, use all character sets" do not support all users in their password generation process. Users have a tendency to remember own-generated passwords better computer-generated ones [18]. Therefore password policies should be such that all users would benefit from them and still be able to generate password with their own style. Sasse et. al. [13] point out that the users should be educated to design stronger passwords and they should be given time and tools for the password generation process. Our study addresses to this point of view.

There exist several studies of passwords creation and memorability. Studies like [1], [2], [17], [18] are examples of password experiments where participants have been students similar to our study. In these studies, when students were let to choose their own passwords, no thorough guidance was given. In our case, much effort was used to teach students how to create a good or a strong password. To motivate users to design strong passwords and eventually make passwords easier to remember, users were allowed to use the designing techniques that are best suited for them. In other words, users were not chained to general password guidelines and for example the use of words was allowed. In large sense this is a part of flexible password policy discussed in [9].

In our study passwords are divided into three different password categories: Non-word passwords, Mixture passwords, and Word passwords. Non-word passwords are character strings, which do not contain any words with any writing styles. However, they can contain letters. Mixture passwords are character strings containing both a word and a non-word part(s), e.g. "?What?!" has two non-word parts ("?" and "?!") around the word part ("What"). Word passwords are strings which are either pure dictionary words, e.g. "password" or readable modifications

Manuscript received May 5, 2010; revised September 20, 2010; accepted September 22, 2010. The work has received financial support from the Research Council of Norway under grant 158777/530.

doi:10.4304/jcp.6.5.969-975

of them e.g. "P@$$W0RD". For each category different password generation guidelines were taught. Password guidelines are derived from the search space reduction computations and are found in author's study [5].

We gave password education for two groups. One group got a classical classroom lecture and the other did a home study based on classroom teaching lecture notes. Both groups were given an access to the password quality measurement tool made by author. The tool uses a questionnaire to derive some simple structures of the passwords. The structure information is then used to compute the quality score of the password. The tool itself is presented in [6].

The remainder of this paper is structured as follows. Section II briefly explains the experiment, Section III summaries the educational part of the study and results are shown in Section IV. Discussion about the study and future work is done in Section V and Section VI concludes the study.

II. Experiment

The study was done with Information Security Bachelor students in their first half semester in 2008 and 2009. Students were taught how to design strong password within three different password categories: Non-word passwords, Mixture passwords, and Word passwords. However, the teaching method was different. When the first group (2008) was taught by using normal class teaching containing lecturing and free question and discussion about the topic, the second group (2009) did an individual home study based on the same lecture notes. Both groups were asked to design a new password after this.

The password categorization was new to students. Therefore, verbal instruction was given to both groups. After the instruction to the password categories, students were also explained how to use the tool provided to measure the password strength. After these two small sessions, students got the first questionnaire. The questionnaire consists of the questions asked by the tool, (translated version of questions in Table II), and also explanation part where students explained how they had constructed the password. With this questionnaire we measured the strength of the current passwords and gained information of the generation process. The education part followed right after the students had delivered their first questionnaire. In total 47 students delivered the first questionnaire. The second questionnaire was carried out one week after. It was similar to the first one, but now the students were asked to use a password they had designed based on previous week teaching session. In total 34 students delivered the second questionnaire. The third questionnaire was carried out again a week after from the second one and answered by 25 students. Now only designed password was asked in order to see how well they were remembered. In addition to these, we asked the home study group fill the questionnaire again after half a year from the education. This fourth questionnaire was identical with the first questionnaire. Only eight students delivered questionnaire back.

TABLE I.
Considered as a single word

Definition	Example
Original dictionary word:	library
Compound dictionary word:	password
Reverse writing:	library → yrarbil
Modifications	
with uppercase letters:	library → LiBRaRy
with digits:	library → l1brary
with special characters:	library → l!br@ry
with uppercases and digits:	library → L1brary
with uppercases and special characters:	library → Libr@ry
with digits and special characters:	library → l1br@ry
with all sets:	library → L1br@ry

TABLE II.
Password quality questions

Whole password	How long is your password?
Word -part	How many words does your password contain? What languages are the words based on? How many letters does the first word contain? How many letters does the nth word contain? How many uppercase letters are there? How many digits letters are there? How many special characters are there?
Non-word -part	How many upper case letters are there? How many lower case letters are there? How many digits are there? How many special characters are there? How many reused characters are there?

III. Teaching Users to Design Good Passwords

A. Password Categories

Passwords can be divided into three categories: Non-word passwords, Mixture passwords, and Word passwords. Non-word passwords are character strings, which do not contain any words with any writing styles. However, they can contain letters. Mixture passwords are character strings containing both a word and a non-word part(s), e.g. "2Glibrary" has a non-word part ("2G") before the word part ("library"). Word passwords are strings which are either pure dictionary words, e.g. "library" or readable modifications of them e.g. "L1br@ry". In our study, we considered modifications shown in Table I as single words. Several examples of the passwords within each category were given to students.

B. A Tool for Password Quality Checking

The tool was given to the students in a form of an Excel-sheet and it was written in Norwegian. Questions of the tool in English are show in Table II. Because passwords can contain both a non-word and a word part, the questionnaire was divided accordingly. The main challenge for student was to understand the separation of these two parts. The strength of the password was not correct if the questionnaire sheet was filled in wrongly. Therefore the instructor's help was important when the tool is used the first time.

TABLE III.
EXAMPLES OF GOOD PASSWORDS IN EACH CATEGORY

Password	Description	Score
Word: $K@1#y@H0$f@R	Based on “Skal øya hos far”, containing 13 characters, 4 words: mod with 3 ul, 2 d, 6 sc	749
Mixture: EeSn#&S0l3!	Based on “Jeg elsker snø og sol”, containing 11 characters, 2 words: mod with 2 uc, 1 d, 1 sc, non-word: 1 lc, 1 uc, 1 d, 2 sc	808
Non-word: 7(3-9f)>K	Based on a math formula, containing 9 characters, non-word: characters from all sets	945

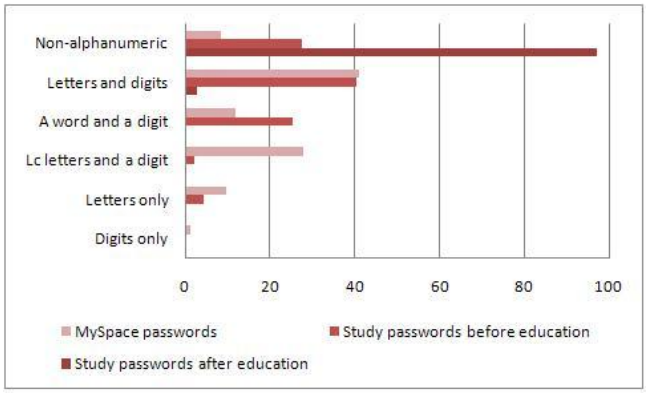

Figure 1. Password structures with common categorization

In [5] we have analyzed the information leakage of passwords when the adversary has an access to the questionnaire answers. Based on these computations the tool used in this study was build. The students were allowed to use the tools freely after the first instruction session. And they were told that a password which scores more than 735 is *a good password* and a password achieving more points than 875 is called *a strong password*. The score points levels are based findings in [4], [5].

C. Password Creation

The students in this study were taught how to create good and strong passwords among each category separately. The guidelines for the password design are again based on the findings in [5].

Word password. Students were taught that a good word password should be longer than 12 characters and it should contain modified words shorter than the half of the length of the actual password. The best modification score will be achieved when all character sets are taken into use when modifying. The words would preferably come from different themes (such as sport and music) and different languages. An example of a good Word password is shown in Table III. The guidelines for Word passwords are following

1) A password should have more than 12 characters.
2) Use many short and modified words.
3) Avoid using same theme.
4) Use variation when modifying.
5) Use different languages and language combination when designing a new password.

Mixture password design. Students were given similar instructions as given for the Word passwords considering the word-part. The strength of the password can be increased when all character sets are taken into use in non-word parts. Table III shows an example of a good Mixture password. The guidelines for Mixture passwords are following

1) A password should be longer than 10 characters.
2) Use either one short, modified word and many extra characters or several short (not the same length), modified words and a few extra characters from large character set.
3) Avoid using same theme.

Non-word passwords The best Non-word passwords are random passwords containing characters from all character set. However, they might be hard to remember. Therefore, students were shown some examples how to generate random-looking passwords in a way that they are easier to remember, etc. mnemonic passwords [12], [17]. Table III shows an example of a strong Non-word password. The guidelines for Non-word passwords are following

1) A password should be longer than 8 characters.
2) Use characters from all character sets, so that more characters come from the large character sets than from the small sets.
3) Vary the number of characters from each set in each construction session.
4) Vary the patterns of character placement.

IV. RESULTS

A. Generation Process

Passwords are often categorized based on what kind of characters they consist of: only digits, only letters, alphanumeric, non-alphanumeric, etc. In the data collected from phishing attack on MySpace 2006 [14], the character mix in passwords were following: 1,3% contained only digits, 9,6% contained only letters, 81% were alphanumeric and the rest 8,3% were non-alphanumeric. Taken a deeper look to the data, among the alphanumeric passwords, a structure pattern was found. 28% of passwords contained lowercase letters having a single digit in the end. 12% contained a single dictionary word having a single digit in the end. 3,8 % of passwords were a single dictionary word.

With similar categorization, the passwords in our study before the education were as follows. 4,3% of passwords contained only letters (being also pure words), 25,5% consisted of a single word and digits and in total 68,1% were alphanumeric. 27,7% of passwords contained at least one symbol. The comparison between MySpace passwords

TABLE IV.
PASSWORD STRUCTURES AND GENERATION PROCESS BEFORE THE EDUCATION (BEFORE), ONE WEEK AFTER THE EDUCATION (AFTER), AND 6 MONTHS AFTER THE EDUCATION (6M). THE CLASSROOM STUDY GROUP IS G1 AND THE HOME STUDY GROUP G2. OTHER ABBREVIATIONS ARE FOLLOWING: LC: LOWERCASE LETTERS, UC: UPPERCASE LETTERS, D: DIGITS, S: SPECIAL CHARACTERS, ALL: ALL CHARACTER SETS, W: WORD, MOD:ALL: MODIFICATION WITH ALL CHARACTER SETS AND NWP: NON-WORD PART. PASSWORDS WITH "HUMAN SELECTED" STUDENTS CLAIMED TO CHOOSE CHARACTERS RANDOMLY. WITH "PASSPHRASE", A MNEMONIC SENTENCE IS USED.

Password Category		Before G1(23)	Before G2(24)	Sum (47)	After G1(16)	After G2(18)	Sum (34)	After 6m(8)
Word		0	2	2	1	0	1	0
	3 w		1	1				
	2 w		1	1				
	4 w, mod:all				1		1	
Mixture		12	12	24	2	7	9	4
	1 w, nwp:d	7	5	12				
	1 w, mod:uc, nwp:d							1
	1 w, mod:all, nwp:d				1		1	
	1 w, nwp:s	1		1				
	1 w, nwp:d,s	2	1	3				
	1 w, nwp:d,s					1	1	
	2 w, nwp:d	1	2	3				
	2 w, nwp:s				1		1	
	2 w, nwp:d,s	1	1	2		2	2	
	2 w, mod:d, nwp:d,s							1
	2 w, mod:uc, nwp:d,s							1
	2 w, nwp:uc,lc,d,s		2	2				
	2 w, mod:all, nwp:uc,d,s					1	1	
	2 w, mod:all, nwp:all					1	1	
	3 w, mod:d, nwp:s							1
	3 w, nwp:uc,lc,d		1	1				
	4 w, mod:all, nwp:s					1	1	
	4 w, mod:all, nwp:uc,lc,s					1	1	
Non-word		11	10	21	13	11	24	4
	Lc,d, Human selected	1		1				
	Uc,s, Alphabetical order				1		1	
	Uc,lc,d, Quickly typed		1	1				
	Uc,lc,d, Human selected	4	1	5				1
	Uc,lc,d, Passphrase	1	1	2		1	1	2
	Lc,d,s, Human selected		1	1				
	Uc,lc,d, Computer gen.	2	5	7				
	All, Human selected		1	1	5	6	11	1
	All, Quickly typed	2		2	1	1	2	
	All, Passphrase	1		1	5	2	7	
	All, Computer gen.				1	1	2	

and passwords which our participants had before and after the education is shown in Figure 1.

In the rest of the paper we use our categorization. With these, 4,3% of passwords were Word passwords, 51,1% were Mixture passwords and the rest 44,7% were Non-word passwords. The password structures before the education session in our study is shown in Table IV in columns "before". In 2008, most of word-parts in the Mixture passwords were modified with uppercase letters remaining word part readable. In 2009, also digits were used together with uppercase letters in word-part modification. Otherwise password generation process was rather similar in both groups.

One week after education (classroom education and home study), the distribution of the password structure and designing process had changed. None of passwords were pure words. One student (2,9%) had used Word-password structure where all words were modified. For the modification all character sets were used. Mixture passwords were 26,5% of all passwords and in 77,8% of them characters from all character sets were used. From all passwords 70,6% were Non-word passwords and 91,7% of these consist of characters from all character sets. The distribution of the password structure after the education is shown in Table IV in columns "after".

In [2], 74 students participated password management practice study. The general password management guidelines were discussed in a classroom. The students' password selection and management practices were analyzed both before and after discussion session. Before the discussion, 46% of students had a word or a word with a digit as a password and 33% of students had a password containing characters from all character sets. After discussion, only 25 students changed their password. Among these 25 students, 20% had a word as a password and 60% used characters from all character sets. In our study, the password change was a mandatory act. After education, no dictionary words were used and in 88,3% of all passwords all character sets were in use. This indicates that the use of specially targeted password guidelines and

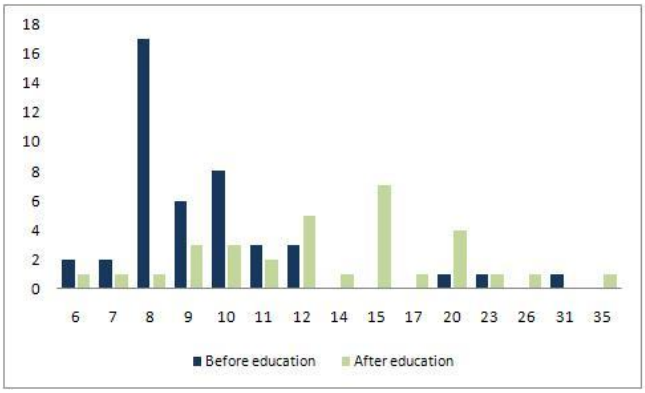

Figure 2. Length distributions

access to the tool, might make the password selection easier and therefore also lead stronger passwords.

Deeper analysis of our study shows, that most of students (81,3%) in the classroom study group (G1) selected Non-word password after class education. Mixture password was only chosen by 1,3% of students. However, in the self-study group (G2), the percent of Mixture passwords was 38,9%, while the rest of the passwords were Non-word passwords. Comparing groups, the group 2 had stretched the variety of the password structure more than the group 1. The large variety of password structures can be thought as a defense against targeted attacks. Before the education an adversary could have done an educated guess successfully based on, for example findings in [14]. After the education the password structures had changed significantly and guessing had become meaningless.

The Table IV shows also the structures of the passwords students had half a year after the education. Half of the students used Mixture passwords and half Non-word passwords. Comparing word parts of the Mixture passwords before and half a year after, it can be seen the education had a slight positive effect. The word parts in the Mixture passwords were indeed modified. However, the special characters were not used in modification as was done one week after the education. The same phenomenon was seen in Non-word passwords. Only one student had used all four character sets when generating the password. Others had only used alpha-numeric characters.

B. Password Length

In MySpace data [14] the most popular password lengths were 6 (15%), 7 (23%), 8 (25%), and 9 (17%) characters. In our case the results were rather similar. 68,7% of passwords had length between 8 and 10 characters. The most popular length was 8 characters (37,8%). The password length distribution before education is shown in Figure 2. Average password length was 9,0 characters for the group 1 (2008), 10,8 characters for the group 2 (2009), and 9,9 characters for both groups together.

After education session, the password length had become more evenly distributed and also the average password length had gotten higher, see Figure 2. This is a good result in two ways. First, the individual passwords have become stronger based on the longer passwords, and the second, the whole password group has become stronger. This means that the adversary knowing the password policy, does not benefit from it. For example, in our University College the password policy states that "minimum password length is 8 characters". Before the education, the adversary had 37,8% chance that student password was 8 characters long. After education, only 5,9% of students had 8 character long password. When looking groups separately, it can be noticed that gap between groups have gotten larger than it was before education. Before education, the group 2 had 1,8 characters longer passwords, and after the education the difference is 4,7 characters.

The average of the password length of the group 2 after half a year from the education had not dropped to the "before education" -level being now 12,1 characters. When comparing passwords with their category guidelines, the passwords were heading to the right directions. Non-word passwords were 8 or more characters long (guideline states "longer than 8" characters), and Mixture passwords were 10 or more characters long (guideline states "longer than 10" characters).

C. Password Strength

When measuring the strength of passwords with our tool, two thresholds were used. Passwords achieving more than 735 points were characterized as good passwords, while passwords more than 875 points were characterized as strong passwords.

Before education the passwords were in general weak. In the group 1, 78% of the passwords were weak, the median score was 476 points, and the mean was 485 ± 144 points with 95% confidence interval. In the group 2, 94% of the passwords was weak, the median was 456 points, and the mean was 585 ± 340 with 95% confidence interval. After the education passwords had gotten stronger. Among the group 1, 20% had a good password and 53% a strong password. The median score was 945 points and the mean was 952 ± 202 points with 95% confidence interval. In the group 2, the percents of the good passwords were 19% and strong passwords 75%. The median was 1234 points and the mean 1262 ± 242 points with 95% confidence interval. This strengthening is due to changes in the password structures, use of all character sets and longer passwords.

The group 2 has higher password quality points both before and after education than the group 1. This can be explained with the length of the passwords. It is also observed that group 2 has always had longer passwords than the group 1. Figure 3 shows how the password strength changed individually. The data shown in the figure consist of the students from both groups who delivered two first questionnaires successfully.

Long term educational effect was measured half a year after the education among the group 2 students. We noticed that the positive effect of the education, which

Figure 3. Scores before and after education with individual changes

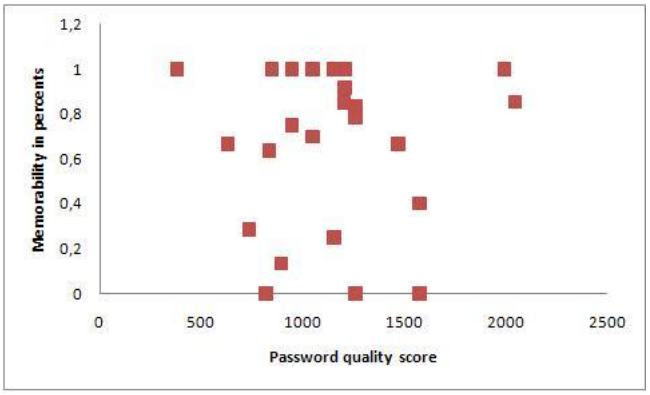

Figure 4. Memorability vs. Quality Score

was so obviously seen after one week from the education, had vanished. In most cases password were weak again. The median had dropped to 544 points and the mean to 590 ± 205 points with 95% confidence interval. The most important reason for strength decreasing was the lack of special characters.

This finding goes along lines with the psychology study of password managements [16] which states that users choose strong passwords only if they are willing to sacrifice convenience. Use of special characters hardens the memority burden of a password and if there are no consequences of choosing weak passwords, users do not bother to create strong ones.

D. Memorability

After a week from password designing date, students were asked to write down their passwords. Students were told not to use their passwords in any applications because the passwords were required to reveal. 48,2% of those who delivered third questionnaire, remembered password either correctly or with 1-2 easily corrected errors. With easily corrected errors we mean errors that are noticed when typed, for example that a password was one character too short. We did not use computers to collect passwords. All questionnaires were on paper and students filled them in a lecture. Taking into consideration that writing a password on a paper is a different process that typing a password on the keyboard, we chose to take into account also 1-2 character errors while password still being a memorabable password.

Here we also find a difference between groups. The group 1 remembered their passwords better than the group 2. Percents being respectively 61,5% and 37,5%. This can be due to the fact that the passwords used by the group 1 were shorter than the passwords used by the group 2.

Figure 4 shows the relations between password memorability and strength. Memorabilty is computed as percents of right characters in a password string. It can be seen that the strong passwords are also memorable.

Zviran and Haga have studied password memorability in several occasions. While studying memorability of cognitive passwords, they used self-generated and system-generated passwords as control group. The recall rates for self-generated passwords after three months were 31% and system-generated 24% [18]. In [19] recall rate for self-selected passwords after three months were 35% and for random passwords 23% All passwords recalled in our study, except one, were self-selected. That one password was computer generated but the student had made the program by himself.

V. Discussion and Future Work

Because the password categorization was new to the students, it had to be thoroughly explained to the students in order to get the password quality measurements correct. However, despite careful explanation, some of the students still find it hard to answer correctly.

We also had to exclude some of the deliveries because the users had used other language than Norwegian. We did not have other languages included our measurement tool, and therefore the password quality scores were not accurate. However, similar instructions as given in password policies can be applied for other languages and the passwords made based on the policies are good or strong passwords.

The number of participants in our study became progressively less to the end. The number of acceptable answers was too small in the end to make the firm decision of which teaching method is the most efficient. It would be interesting to see how the password strength would change if the password guidelines shown in this paper were always visible to the users when changing a password. This would remind users of good password generation habits, and the effect of the continuous education could be measured.

VI. Conclusion

In this study, we taught two student groups how to design strong passwords in three different password categories: Word passwords, Mixture passwords and Non-word passwords. For each category different password generation guidelines were given. The education differed between groups. One group received a classical classroom lecture session and the second studied the same material at home as a self-study. In both cases, the passwords designed right after the education, were much stronger.

Not only password length got longer, but also all character sets were taken into password designing processes.

The most important finding after the password education was that password structure changed. The variation among structures had increased, and the distribution of password structure and also password length had become closer to the uniform distribution. The large variety of password structures and lengths is a good defense against targeted attacks.

However, one-time education did not help students to generate good passwords after half a year from the education. Within this timeframe the password guidelines of the high school had not changed and student had not received any remainders of strong passwords. We asked the home study group to answer to the fourth questionnaire. Only eight students answered. Despite the small number of delivering, a tendency could be derived. The students had problems to add special characters to their passwords. Passwords were also slightly shorter than right after the education. Both these reasons influenced on password strength by making it weak again.

In order to make firm predictions of which teaching style gives better results, the number of students in each group should have been higher. However, based on the results in this study, the self study group achieved larger password structure variation, longer passwords and higher quality points. This indicates that the self study is as sufficient as a traditional class teaching.

When considering memorability, the study supports the idea that self generated passwords are easier to remember than computer generated. In our study all remembered passwords, except one, were self generated. The study also indicates that passwords made based on different policies among different password categories are at least as memorable as other passwords.

ACKNOWLEDGEMENTS

The author is grateful to the students participating this study, to Nils Kalstad Svendsen for guiding the self study group and to Einar Snekkenes for valuable feedback. This work is supported by the Research Council of Norway, grant 158777, Authentication in a health service context.

REFERENCES

[1] A. Brown, E. Bracken, S. Zoccoli, and K. Douglas. Generating and Remembering Passwords. *Applied Cognitive Psychology*, 18:641–651, 2004.

[2] C. P. Garrison. Encouraging good passwords. In *Proceedings of InfoSecCD Conference*, pages 109–112. ACM Press, 2006.

[3] E. Gehringer. Choosing Passwords: Security and Human Factors. In *Proceedings of ISTAS'02*, pages 39–373, 2002.

[4] K. Helkala and E. Snekkenes. A method for ranking authentication products. In *Proceedings of the International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008), July 8-9, Plymount, UK*, pages 80–93, 2008.

[5] K. Helkala and E. Snekkenes. Password generation and search space reduction. *Journal of Computers*, 4, Issue 7:663–669, 2009.

[6] Kirsi Helkala. An educational tool for password quality measurements. In *Proceedings of Norwegian Information Security Conference*, pages 69–80. Tapir Akademisk Forlag, 2008.

[7] Ann-Marie Horcher and Gurvirender P. Tejay. Building A Better Password: The Role of Cognitive Load in Information Security Training. In *Proceedings of IEEE International Conference on Intelligence and Security Informatics, ISI*, pages 113–118, 2009.

[8] Information Technology Services, The Pennsylvania State University. Password Policy. `its.psu.edu/policies/password.html`, 2006.

[9] P. Inglesant and M. A. Sasse. The True Cost of Unusable Password Policies: Password Use in the Wild. In *Proceedings og the CHI 2010*, pages 383–392. ACM Press, 2010.

[10] ISO. *NS-ISO/IEC 17799:2001*.

[11] Frank H. Katz. The Effect of a University Information Security Survey on Instruction Methods in Information Security. In *Proceedings on Information Security Curriculum Development Conference*, pages 43–48, 2005.

[12] C. Kuo, S. Romanosky, and L.F. Cranor. Human selection of mnemonic phrase-based passwords. In *Proceedings of the second symposium on Usable privacy and security*, volume 149 of *ACM International Conference Proceeding Series*, pages 67–78. ACM Press, 2006.

[13] M.A. Sasse, S. Brostoff, and D. Weirich. Transforming the "weakest link" - human/computer interaction approach to usable and effective security. *BT Technol*, 19(19):122–131, 2001.

[14] B. Schneier. Crypto-Gram Newletter: Real-World Passwords. `www.schneier.com/crypto-gram-0612.html`, December 2006.

[15] Robin Snyder. Ethical Hacking And Password Cracking: a Pattern For Individualized Security Exercises. In *Proceedings on Information Security Curriculum Development Conference*, pages 13–18, 2006.

[16] L. Tam, M. Glassman, and M. Vandenwauver. The psychology of password management: a tradeoff between security and convenience. *Behaviour and Information Technology*, 29(3):233–244, 2010.

[17] J. Yan, A. Blackwell, A. Anderson, and A. Grant. The Memorability and Security of Passwords - Some Empirical Results. Technical Report 500, Computer Laboratory, University of Cambridge, 2000.

[18] M. Zviran and W.J. Haga. User authentication by cognitive passwords: an empirical assessment. In *Proceedings of the 5th Jerusalem Conference on Information Technology*, pages 137–144, 1990.

[19] M. Zviran and W.J. Haga. A Comparison of Password Techniques for Multilevel Authentication Mechanisms. *Computer Journal*, 36(3):227–237, 1993.

BIOGRAPHY

Kirsi Helkala is holding a PhD degree in information security from University of Oslo, Norway, 2010. Currently she is an associated professor at Gjøvik University College, Norway. Her research topic is personnel authentication.