Human Generated Passwords – the Impacts of Password Requirements and Presentation Styles

Paul Y. Lee and Yee-Yin Choong

National Institute of Standards and Technology
100 Bureau Drive, Gaithersburg, MD 20899, USA

{paul.lee, yee-yin.choong}@nist.gov

Abstract. The generation stage of the user password management lifecycle is arguably the most important yet perilous step. Fulfilling minimum length and character type requirements while attempting to create something memorable can become an arduous task, leaving the users frustrated and confused. Our study focuses on two areas – password requirements and formatting, and examines the differences in user performance to understand the human password generation space. The results show a clear drop in performance when users generate passwords following a complex rule set as opposed to a simple rule set, with fewer passwords, more errors, and longer times for rule comprehension and password generation. Formatted presentation helps reduce cognitive load in reading complex password rules and facilitates the comprehension. Findings from this study will contribute to a better understanding of the user password generation stage and shed light on future development of password policies balancing security and usability.

Keywords: password generation, cyber security, password policy, usability.

1 Introduction

Password based authentication plays a critical role in information access, controlling everything from bank accounts to web forums and everything in between. Unfortunately, passwords are easy targets and thus are constantly under attack from many cracking methods. The consequences of these attacks can vary from minor annoyances such as having to reset a password, to extremely severe if someone manages to access personal data or financial information. These cracking attempts are made easier by the fact that an overwhelming proportion of users are creating passwords that only contain lowercase letters if no other character types are required [1]. Though many password policies do require users to create passwords containing multiple character types and of a certain length, this introduces usability concerns such as password creation difficulty and memorability.

When creating a password, the user's ultimate goal is to create a text string that is both memorable and sufficiently secure. However, the additional creation criteria can drastically slow down the generation process as the user needs to ponder what items they can include to satisfy the requirements while still making the password easy to recall [2]. What is needed is an examination of what actions can be taken to alleviate some of the usability issues that arise from stringent password requirements. Here we present lab-based user-generated data and examine the differences in password generation performance when users are faced with different requirements and instruction formats, as well as character distribution patterns in user-generated passwords.

2 Background

As IT-based technologies become more and more integrated in our lives, the number of accounts and passwords a person must keep track of increases. The average person has multiple accounts, ranging from email and banking to the more recent areas of social media and mobile applications. Weak passwords for these accounts could result in increased security risks including unauthorized access to personal information and finances, activity monitoring, and the attacker posing as the target in online interactions. Consequently, large swathes of research have been dedicated to the area, analyzing not only the security of passwords (e.g., [3], [4], [5], [6]), but also users' password selection behaviors (e.g., [7], [8], [9]).

Of the three stages in the password management lifecycle [10], our paper focuses on the first – the password generation stage. In this stage, users need to comprehend the password rules presented, explore options of characters to use, and finally compose a text string to satisfy the rules. It is important to understand what factors are at play here, as the subsequent maintenance and authentication stages rely on the generation stage to be both secure and usable. Several methods of facilitating password generation have been proposed, including mnemonics, passphrases, and various probes into graphical authentication. Though research in these areas shows varying levels of promise (e.g., [5], [11,12]), their real world application is limited.

One of the more commonly implemented methods of regulating the password generation stage is dynamic compliance checking. This approach programmatically checks for adherence of the character-based passwords created by a user to predefined rules. These rules often include minimum and maximum string lengths, mandatory inclusion/exclusion of certain character types, and restricting the use of certain words. These password rules are to ensure that users create passwords that fall within a range of acceptable security levels, as users tend to rarely use special characters (non-letter and non-number) unless explicitly required to do so (e.g., [1], [5]).

This study has two objectives. The first is to investigate the password generation space in relation to the length and complexity of password rules. Examining how these rules affect the makeup of passwords such as character distribution and placement patterns will help us better understand how password requirements constrain human-generated passwords. The second is to explore the effects the presentation of the password rules may have on users' password generation performance. Understanding and quantifying the cognitive processes and strategies used during password gen-

eration will support the ultimate goal of finding an optimal combination of length and complexity requirements, and presentation style that balances security and usability.

Past research that explores the password generation space asks users to create limited number of passwords [e.g., 5] or instructs users to create passwords for specific accounts [e.g., 2,3]. In contrast, this study examines password composition and creation behavior when users are given a longer period of time to generate passwords with only rule complexity and presentation style as factors. Giving participants more time to create passwords allows for an in-depth investigation into generation patterns, while not focusing on creating passwords for specific accounts avoids potential changes to creation behavior due to pre-conceived notions that certain accounts require more secure passwords. A limitation of the study is that users were asked to generate multiple passwords at one time in a lab setting.

Research has found that formatted text can facilitate online reading such as improving comprehension and reading efficiency, compared to block text (e.g., [13, 14]. To understand the potential effects of how password rules are presented, we formed the following hypothesis: users with password requirements presented in a formatted manner will have better password generation performance than users with password requirements presented in an unformatted manner.

3 Method

3.1 Participants

Eighty-one participants were recruited from the metropolitan area of Washington, D.C., the United States. The participants ranged in ages from 18 to 69 years old (*Mean* = 35.1). Approximately 47% were male and 53% were female and represented diverse education and occupation backgrounds. Qualified participants had to be familiar with typing using a standard keyboard.

3.2 Apparatus[1]

An experimental program was developed in Python version 3.3.2 for data collection. The program is running on a desktop computer (Windows 7 Enterprise, Intel® Core i7-3770 CPU @ 3.40GHz, with 16.0 GB RAM) with a 24-inch LCD monitor, a standard keyboard, and a 2-button USB optical mouse with scroll wheel.

[1] Specific products and/or technologies are identified solely to describe the experimental procedures accurately. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products and equipment identified are necessarily the best available for the purpose.

3.3 Experimental Design

To investigate the password generation space, we gave each participant two sets of password rules and asked them to generate as many passwords as possible within set time limits. The password rule sets are with two levels of complexity. The simple rule set only requires minimum length of 6 characters. For the complex rule set, we chose stricter rules commonly used in organizations controlling their employees' access or used for personal accounts protecting data of more sensitive nature such as banking or credit cards. The complex rules include minimum length, mixed-case alphabets, numbers, and special characters (Table 1).

To test the proposed hypothesis, the password rules were presented in different styles: formatted and unformatted. There are many existing guidelines on text formatting for online reading and comprehension. As a starting point to explore the effects of password requirement presentation styles, we only employed minimal formatting differences by turning an unformatted text into bullets and adding line breaks. This condition is between-subject, i.e., 40 participants were presented with formatted password rules and 41 participants were presented with unformatted password rules. To eliminate potential order effects, the sequence of receiving the two rule sets was counter-balanced, i.e., half of the participants (41) in a between-subjects conditions (formatted or unformatted) started with the complex set, followed by the simple set; the other half (40) started with the simple set, followed by the complex set.

Table 1. Experimental Design

	Password Rules	
Presentation Style	Complex	Simple
Formatted	You have 12 minutes to generate as many passwords as you can. Your password **must have**: • at least 12 characters • at least 1 uppercase letter (A to Z) • at least 1 lowercase letter (a to z) • at least 1 number (0 to 9) • at least 1 symbol. Your password **must not**: • have 5 occurrences of the same character • contain any dictionary words.	You have 8 minutes to generate as many passwords as you can. Your password **must have**: • at least 6 characters. You can use **any characters** that can be typed on a standard keyboard. Password tip: It is recommended that you use a combination of upper and lower case letters, numbers and symbols.
Unformatted	You have 12 minutes to generate as many passwords as you can. Your password must be a minimum of twelve characters in length. Each password must contain at least one of each of the following types of characters: uppercase alphabetic (A to Z), lowercase alphabetic (a to z), numberic (0 to 9), and symbols. Your passwords cannot contain any dictionary words. Your passwords cannot have five occurrences of the same character.	You have 8 minutes to generate as many passwords as you can. You need to create a password of minimum 6 characters long. You can use **any characters** that can be typed on a standard keyboard. Password tip: It is recommended that you use a combination of upper and lower case letters, numbers and symbols.

Detailed data were logged programmatically including: number of passwords generated, time spent on password generation, and key presses. All timing data were

measure in seconds (s). The final experimental design with different password rule presentation styles is in Table 1.

3.4 Procedure

Participants performed the study individually. Upon arriving at the study facility, the participant was greeted and briefed about the study by the researcher. Each participant was assigned an identification number and randomly assigned to a condition (formatted or unformatted). The researcher started the experimental program, left the testing room, observed the session in an adjacent control room via video feeds, and communicated with the participant using microphones and speakers if necessary.

The experimental program presented the first password rule set and instructed the participant to generate as many passwords as possible according to the requirements within a pre-determined time limit (12 minutes for the complex rules and 8 minutes for the simple rules). Participants were informed that they do not have to memorize the passwords generated. Repeated passwords were rejected. Upon finishing the first rule set, the participant received a second rule set and performed the generation task.

After the password generation tasks, participants completed a questionnaire regarding their perception on the difficulty of the password generation tasks and on the strength of the password rule sets.

4 Results and Discussion

4.1 Descriptive Statistics

The 81 participants created 8,165 compliant passwords in total (3,138 complex; 5,026 simple), averaging 100.8 passwords per participant (STD = 57.04). On average, a participant generated 38.74 complex passwords and 62.05 simple passwords. Detailed performance metrics are summarized in Table 2.

Table 2. Password Generation Performance

Complex Passwords	**Mean**	**STD**	**Median**	**Min**	**Max**	**Sum**
Number of passwords	38.74	21.93	34.00	3	106	3138
Avg. password length	14.23	1.67	13.72	12.03	19.68	n/a
Avg. generation time	29.25	32.00	21.18	6.79	240.00	n/a
Time to 1st key press	23.98	14.58	20.59	4.65	90.00	n/a
Time to 1st password	57.33	58.69	43.96	4.30	351.62	n/a
Time to 1st compliant password	82.65	103.71	50.45	14.93	734.39	n/a
Simple Passwords	**Mean**	**STD**	**Median**	**Min**	**Max**	**Sum**
Number of passwords	62.05	39.57	52.00	8	205	5026
Avg. password length	9.15	2.27	8.74	6.05	20.17	n/a
Avg. generation time	11.54	9.21	9.23	2.34	60.00	n/a
Time to 1st key press	14.35	7.90	12.81	2.15	44.08	n/a
Time to 1st password	22.17	11.20	6.69	58.78	19.86	n/a
Time to 1st compliant password	22.28	11.63	19.86	6.57	58.76	n/a

The demanding nature of the complex rule set made for participants taking longer to reach milestones such as hitting the first key or creating their first compliant password. On average, it took participants 82.65 s to create their first compliant complex password. Further breaking down steps taken in these 82.65 s, it took users 23.98 s on average to make their first key press after being presented with the complex rules. Then, it took additional 33.35 s to attempt their first password, and another 25.32 s to create their first compliant password. In contrast, when faced with the simple rules, participants took an average of 14.35 s to press the first key, an additional 7.82 s for first password attempt, and just 0.11 more seconds to complete their first compliant password. Overall it took participants 17.71 s longer to generate a compliant complex password (29.25 s) than to generate a compliant simple password (11.54 s). Finally, due to the differences in length requirements (at least 12 for complex; at least 6 for simple), the passwords generated from complex rules average 14.23 characters in length while passwords generated from simple rules average 9.15 characters in length.

During the password generation tasks, the experimental program provided instantaneous visual feedback on the compliance of the text string being typed. The text entry field started with a red background (i.e., non-compliant) and changed to a green background (i.e., compliant) at the moment when the password string adhered to the rule set. Once minimum compliance was met, the participants had the option to submit the string or keep typing until they were satisfied. Because of this real-time dynamic compliance checking feature, there were not many non-compliant passwords (i.e., errors) submitted. Twenty-six participants did not generate any non-compliant passwords and the other fifty-five participants generated at least one non-compliant password. We also recorded the number of retry attempts submitted after an error occurred until a compliant password was generated. The results from those fifty-five participants are summarized in Table 3. On average, participants made about twice as many errors with the complex rule set and took three more attempts to recover from the errors, as compared to the performance with simple rule set.

Table 3. Errors and Retry Attempts

Complex Passwords	**Mean**	**STD**	**Median**	**Min**	**Max**
Errors	3.07	4.41	2.00	0	26
Retry Attempts	4.49	7.46	2.00	0	33
Simple Passwords	**Mean**	**STD**	**Median**	**Min**	**Max**
Errors	1.45	2.955	1.00	0	15
Retry Attempts	1.44	3.11	1.00	0	17

4.2 Password Generation Space

4.2.1 Character Distribution

To understand the content of the user-generated passwords, we split all characters into four types: lowercase letters, uppercase letters, numbers, and special characters. Table 4 shows the character distribution of the 3,138 complex passwords and the 5,027 simple passwords.

Lowercase letters far outstrip all other character types in both rule sets, representing 56.15% of characters in complex passwords and 69.37% of characters in simple passwords. The large proportion of lowercase letters in simple passwords is likely due to the rule set only requiring at least six characters of any type.

Table 4. Character Type Distribution

Character Type	Complex Passwords		Simple Passwords	
	Frequency	Percentage	Frequency	Percentage
Lowercase Letter	25786	56.38%	30993	69.39%
Number	8865	19.60%	7565	16.94%
Uppercase Letter	5968	13.05%	3766	8.43%
Special (Non-alphanumeric)	5020	10.98%	2344	5.25%

Previous research has reported that if character type use is not enforced, users are much more likely to stick to lowercase letters [1]. This rise of lowercase letters in simple passwords does not affect character type frequency ranking, as both datasets have lowercase letters as the most common character type, followed by numbers, then by uppercase letters and special characters. Further, due to the lack of character type quotas in the simple rule set, the occurrences of numbers, uppercase letters, and special characters are all lower than those in complex passwords. More interesting are the results pertaining to the complex dataset, as the rules closely mimic many real world generation guidelines and thus the results are more relevant in today's password creation landscape.

Table 5. Ten Most Common Characters in Complex Passwords, based on Character Types

Lowercase	Frequency	Percentage	Uppercase	Frequency	Percentage
e	2478	9.61%	S	369	6.18%
a	2006	7.78%	L	354	5.93%
o	1864	7.23%	D	340	5.70%
r	1836	7.12%	T	330	5.53%
s	1831	7.10%	C	319	5.35%
n	1650	6.40%	F	310	5.19%
t	1621	6.29%	W	308	5.16%
i	1468	5.69%	M	305	5.11%
l	1161	4.50%	P	296	4.96%
h	1094	4.24%	A	289	4.84%
Number	**Frequency**	**Percentage**	**Special**	**Frequency**	**Percentage**
1	1328	14.81%	!	895	17.83%
2	1175	13.11%	#	569	11.33.%
3	1146	12.78%	*	525	10.46%
0	1088	12.14%	@	499	9.94%
4	927	10.34%	$	401	7.99%
9	824	9.19%	%	218	4.34%
5	769	8.58%	SPACE	218	4.34%
8	697	7.77%	.	192	3.82%
7	533	6.17%	&	188	3.75%
6	458	5.11%	^	162	3.23%

After splitting up the character distribution by character type, we further explored the data by examining the most common characters from each category, as seen in Table 5. We compared specific alphabet frequencies to their occurrences in continuous English text to see if the password generation environment had any effect. Nine of the top ten lowercase letters (e, a, o, s, r, n, t, l, and h) in complex passwords appear in the top ten most common letters in the English language (e, t, a, o, n, i, r, s, and h) [15]. The top ten uppercase letters in Table 5 do not fair quite as well, with only S, L, T, and A matching up. They do match much more closely with the top ten most common starting letters in the English language (t, o, a, w, b, c, d, s, f, and m) [15], with eight matches total. A possible explanation for this difference is that during the study sessions, we observed many participants used English-like words in their passwords. With the need for an uppercase letter in a valid complex password, many participants capitalized the first letter of these English-like words to fulfill the requirement.

The top three numbers are 1, 2, and 3, which follows the natural numerical ordering, followed by 0 which is the last digit of the number row on the keyboard. Speical characters follow a similar distribution, with ! (SHIFT-1), @ (SHIFT-2), and # (SHIFT-3) appearing in the top four in Table 5.

4.2.2 Complex Password Patterns

In addition to the character distribution, we examined character type positioning to determine if the generated passwords followed any particular placement pattern. We again focused our analysis on compliant complex passwords. Figure 1 displays the overall character type distribution relative to their position for password lengths of 12 through 18. This range accounts for 92% of all complex passwords created.

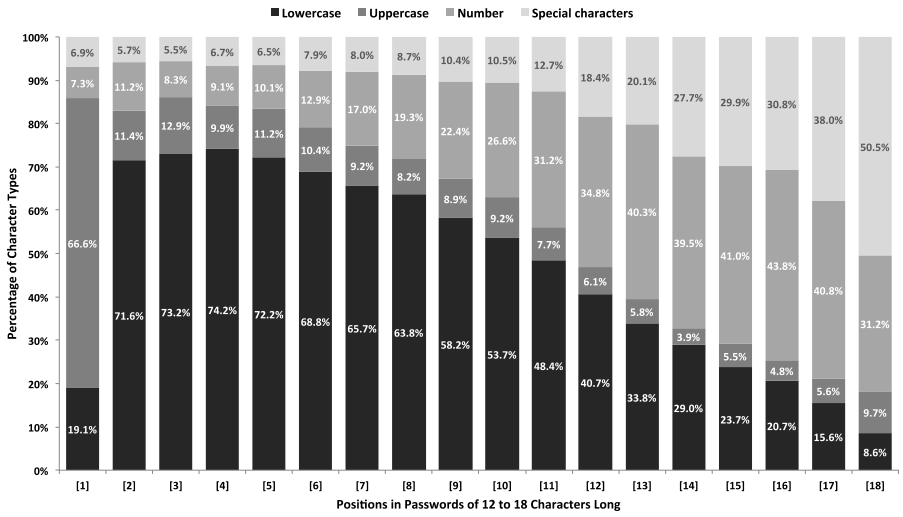

Fig. 1 Character Type Distribution for Specific String Positions

Uppercase letters dominate the first position of the password string, accounting for 66% of all characters. This correlates with the statement earlier that many participants capitalized the English-like words in their passwords, which were often the first por-

tion of the string. However the rate sharply drops off to 11% at the second position and slowly decreases toward the last position. Lowercase letters start at a much more modest 19%, before rising to 71% in position 2. This 71% trend holds steady for four positions (2 to 5) before the rate begins to decline at position 6 with an average rate of 5% per position, before finally ending at 8.6%. Numbers and special characters begin at about 7%, but the percentage of numbers begins to increase at position 6, as opposed to special characters which stay relatively steady until position 12 where they begin to rise. Numbers are the predominant character type from position 13 and stay so until the last position in which special characters make up half of the character distribution.

This pattern of uppercase, lowercase, numbers, and special characters positioning was found consistently when examining the data from specific password lengths. We observed that, when generating passwords, participants would exceed the minimum 12-character requirement. Thus, any particular generation pattern used would hold steady regardless of password length. In addition, we found that this pattern closely follows the rule sequence as presented in the complex password requirements in Table 1. It is of great interest to investigate in future research whether the character positioning changes if the rules are presented in different order.

4.3 Hypothesis Testing

We set the α of all tests for statistical significance to 0.05 for testing the hypothesis on whether users with formatted rule presentation have better password generation performance over users with unformatted presentation. First, we performed a check on all data against the assumptions for parametric statistical tests. Since all of the data violate the normality and equal-variance assumptions, non-parametric tests were used. Table 8 summarizes the performance for each condition group.

Table 8. Impacts of Presentation Styles on Password Generation Performance

Performance	**Presentation Styles**									
	Formatted (n=40)					**Unformatted** (n=41)				
	Mean	STD	Median	Min	Max	Mean	STD	Median	Min	Max
Total number of passwords	108.85	58.26	100.00	29	300	92.93	54.83	82.00	11	253
Complex passwords										
Number of passwords	39.48	21.00	36.00	8	95	38.02	23.02	32.00	3	106
Avg. generation time	25.31	18.02	20.00	7.58	90.00	33.10	41.24	22.50	6.79	240.00
*Time to 1st key press**	21.20	13.84	18.55	4.65	75.39	26.70	14.95	24.70	8.27	90.00
Time to 1st compliant password	79.78	122.24	47.34	17.48	734.39	85.45	83.23	52.53	14.93	333.58
Simple passwords										
*Number of passwords**	69.38	41.67	58.00	12	205	54.90	36.51	47.00	8	186
*Avg. generation time**	9.68	6.84	8.28	2.34	40.00	13.35	10.82	10.21	2.58	60.00
Time to 1st key press	14.67	7.96	13.82	2.70	35.54	14.04	7.93	12.25	2.15	44.08
Time to 1st compliant password	22.56	12.37	20.24	6.57	58.76	21.99	11.00	19.50	9.33	53.92

* indicates statistically significant.

We performed the Mann-Whitney Independent Samples U test to examine the impacts of presentation styles on participants' performance. The hypothesis is partially

supported with significant differences found on three performance variables: *Time to first key press for complex passwords* (U=584.0, z= -2.229, effect size (r) = -0.25), *Number of simple passwords generated* (U=612.5, z= -1.96, effect size (r) = -0.22), and *Average generation time of simple passwords* (U=612.5, z= -1.96, effect size (r) = -0.22). The results show that formatted presentation has positive effects on simple password generation, i.e. more passwords and shorter generation time.

Also, when participants were faced with the stringent complex password requirements, it took them 33% longer time to start the password generation activity (i.e., time to 1st key press) with unformatted presentation. This indicates that the formatted presentation helped reduce participants' cognitive load in reading the password rules and facilitated the comprehension.

4.4 Perceptions on Password Rule Strength and Generation Difficulty

Participants were asked to rate their perception using a 5-point semantic distance scale on: the strength of the password rules in protecting their accounts on (1 – Very Weak and 5 – Very Strong); and the difficulty of password generation (1 – Very Difficult and 5 – Very Easy), for each password rule set. The results are summarized in Table 9.

Table 9. Perceptions on Password Rule Strength and Generation Difficulty

Perception Ratings	Mean	STD	Median	Min	Max
Strength_Complex	4.27	0.73	4.00*	2	5
Strength_Simple	2.77	1.13	3.00*	1	5
Difficulty_Complex	2.68	1.08	2.00*	1	5
Difficulty_Simple	4.19	0.94	4.00*	1	5

* indicates statistically significant.

We used the Wilcoxon Signed Ranks Test, within-subject comparisons, to examine whether each participant had different perceptions on different password rules. There are significant differences on the perceptions of the strength of the password rules and the difficulty of password generation tasks. In general, participants understand that the complex password rules provide stronger protection (Mdn=4) over their accounts than the simple password rules do (Mdn=3). However, it is more difficult to generate passwords that are compliant with stringent and complex password rules (Mdn =2).

Participants with formatted presentation style tend to perceive the password generation task a little more easily than the participants with unformatted style for both the complex rules and the simple rules, as summarized in Table 10. Mann-Whitney U Test was used to examine the impacts of presentation styles on participants' perceptions. Only the perception on the strength of simple password requirements is found statistically significant. Interestingly, participants with the unformatted simple rules perceive the rules as being stronger as opposed to the formatted rules. While more research is needed, a plausible explanation is that the unformatted presentation makes it harder for participants to separate each requirement from the others, which then triggers a false perception of added complexity and strength in the rules.

Table 10. Impacts of Presentation Styles on Participants' Perceptions

Perception Ratings	Presentation Styles					
	Formatted (n=40)			**Unformatted** (n=41)		
	Mean	STD	Median	Mean	STD	Median
Strength_Complex	4.25	0.71	4.00	4.29	0.75	4.00
Strength_Simple	2.50	0.99	2.00*	3.02	1.21	3.00*
Difficulty_Complex	2.88	1.04	2.50	2.49	1.10	2.00
Difficulty_Simple	4.35	0.77	4.50	4.02	1.06	4.00

* indicates statistically significant.

5 Conclusion

Given the near universal reliance on password based authentication methods, our study aimed to better understand the human generated password space as it relates to password requirements and formats. Users' password generation performance with the complex rule set was consistently lower, e.g., longer times for rule comprehension, longer times for password generation and fewer passwords generated, compared to their performance with the simple password rule set. Additionally, participants made twice as many errors when generating complex passwords, and took three times the amount of retries until a valid password. With close examination on the passwords from the complex rule set, it is clear that the stringent nature of the rules does not expand the password generation space much beyond those commonly used alphabetical letters in English language.

This study explored the potential impacts of password rule presentation styles on users' password generation performance. Although the hypothesis was only partially supported, the results show general trends of better performance, e.g., taking shorter time and generating more passwords, from formatted rule presentation. Given the fact that the formatting manipulation in this study was only adding some organization (such as bullets and line breaks) to an unformatted block of text, it would be of great interest to investigate the impacts on password generation performance with more elaborate formatting manipulations such as changing phrasing, plain language, reordering rules, and changing text styles (e.g., font family, font size, bolding).

This paper provides findings from our preliminary analyses on the data collected from the study. We intend to perform more in-depth analyses to fully understand how participants approached the password generation tasks when faced with different password rules. It is also of great interest to investigate whether there are relationships between the demographic data (e.g., age, education, self-reported computer proficiency) and participants' password generation performance. We expect the research will shed light on the development of password policies, shoring up the difficulty balancing security and usability.

References

1. Florencio, D., Herley C.: A Large-Scale Study of Web Password Habits. In: Proceedings of the 16th International Conference on World Wide Web, pp. 657-666. ACM, New York (2007)
2. Proctor, R., Lien, M., Vu, K., Schultz, E., Salvendy, G.: Improving computer security for authentication of users: Influence of proactive password restrictions. Behavior Research Methods, Instruments, & Computers, 163-169. (2002)
3. Vu, K., Proctor, R., Bhargavspantzel, A., Tai, B., Cook, J., Eugeneschultz, E.: Improving Password Security and Memorability to Protect Personal and Organizational Information. International Journal of Human-Computer Studies, 744-757 (2007)
4. Weir, M., Aggarwal, S., Collins, M., Stern, H.: Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords. In: Proceedings of the 17th ACM Conference on Computer and Communications Security, pp. 162-175. ACM, New York (2010)
5. Yan, J., Blackwell, A., Anderson, R., Grant, A.: Password memorability and security: Empirical results. IEEE Security & Privacy Magazine, 25-31 (2004)
6. Florencio, D., Herley, C., Oorschot, P.: An Administrator's Guide to Internet Password Research. In: 28th Large Installation System Administration Conference. Usenix, Washington (2014)
7. Roman V., Y.: Analyzing User Password Selection Behavior for Reduction of pass-word space. In: Proceedings 2006 40th Annual IEEE International, pp. 109-115. IEEE, New Jersey (2006)
8. Jakobsson, M., Dhiman, M.: The Benefits of Understanding Passwords. In: Proceedings of the 7th USENIX Workshop on Hot Topics in Security. Usenix, Washington (2012)
9. Grawemeyer, B., Johnson, H.: How Secure Is Your Password? Towards Modelling Human Password Creation. In: *Proceedings of the First Trust Economics Workshop*, pp. 15-18 (2009)
10. Choong, Y.: A Cognitive-Behavioral Framework of User Password Management Lifecycle. In: HCI International 2014, pp 127-137 (2014)
11. Jermyn, I., Mayer, A., Monrose, F., Reiter, M., Rubin, A.: The Design and Analysis of Graphical Passwords. In: 8th USENIX Security Symposium, pp 1-1, (1999)
12. Keith, M., Shao, B., Steinbart, P.: A behavioral analysis of passphrase design and effectiveness. Journal of the Association for Information Systems, *10*(2), 2, (2009)
13. Walker, R. C., P. Schloss, C. A. Vogel, A. S. Gordon, C. R. Fletcher, S. Walker.: Visual-syntactic text formatting: theoretical basis and empirical evidence for impact on human reading. In: Professional Communication Conference, pp 1-14 (2007)
14. Yu, C.-H., Miller, R.C.: Enhancing web page readability for non-native readers. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp 2523-2532 (2010)
15. Bourne, C., Ford, D.: A Study of the Statistics of Letters in English Words. Information and Control, 48-67 (1961)