정 보 보 호 학 회 지
제28권 제1호, 2018. 2

Survey on Current Password Composition Policies

Simon S. Woo*, Kyeong Joo Jung**, Bong Jun Choi***

Abstract

Textual passwords are widely used for accessing online accounts. Despite the problems of current textual passwords, research has shown that there is no other strong alternatives for a textual password due to its simplicity. There has been significant research to make passwords more secure and usable through password composition policies, password managers, password meters, and multi-factor authentications. In this paper, we focus on several key research that investigates and analyzes widely used password composition policies, and summarize the latest research which aims to improve current password composition policies.

Ⅰ. Introduction

A textual password is a composed of characters, symbols, or numbers for authenticating user's identity for various online accounts and systems. Due to its simplicity, a textual password has been widely adopted for many systems. However, attacks on textual passwords such as stealing or eavesdropping have been greatly increased with various online and offline attacks. Therefore, it is critical for users to create strong passwords that can be resistant to these online and offline attacks. In order to help and guide users to create strong passwords, password composition policies have been used, which password policies typically require a minimum number of characters and/or enforcing the use of special characters, or uppercase/lowercase letters. The most popular password policy is a 3class8 policy, which requires at least 8 characters and minimum 3 character classes (lowercase letters, uppercase letters, digits, and special characters). The 3class8 policy has been widely adopted by many websites to strength user-created passwords. However, several research[1-3] has shown that current password composition policies are not effective in improving strength and memorability.

In this paper, we summarize results from several research investigating problems with current password composition policies, and present the latest research for addressing and improving current password composition policies.

The paper is organized in the following way: In Section II, we describe the research shows the problems with current password composition policies. In Section III, we present the latest research that attempts to address and improve current password composition policies. We discuss about the different proposed approaches in Section IV, Lastly, we end this paper with our conclusion in Section V.

본 연구는 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구입니다.(No. NRF-2017R1C1B5076474)
* 교신전자, 한국뉴욕주립대학교 컴퓨터과학과(SUNY, Korea) (simon.s.woo@sunykorea.ac.kr)
** Stonybrook University, SUNY Korea, (kyeongjoo.jung@stonybrook.edu)
*** Stonybrook University, SUNY Korea, (bjchoi@sunykorea.ac.kr)

Ⅱ. Problems with Current Password Composition Policies

Currently, there are several problems with password composition policies.

Inconsistency: One of the major problems with password composition policies is that they are inconsistent across different websites. Some websites enforce 3class8 policy, while others only require 2class8 policy. Even worse, using the same 3class8 policies, some websites only accept certain subsets of special characters and do not accept certain characters (e.g. "%"), while others accept all special characters. Therefore, when users create passwords for websites, different policies can cause users' frustration, and confusion. This can potentially lead users to bad practices such as writing passwords down. Also, different policies result in different password strength. It is clear that typically website administrators are not fully consider, understand, and control the impacts of different policies with their resulting strength and usability.

However, there is a possible advantage of having different password composition policies for preventing password reuse. For example, each website enforces its own password composition policy. Then, users are forced to create different passwords. However, as shown in Ur et al.[3], users make predictable changes from their one password to another password. Hence, the benefit of having different password composition policies is easy to achieve.

Also, some researchers advocate[1] that password policies should be context-aware, meaning websites require stronger strength such as banks need to have more stringent policies than websites do not such as social networking sites. However, currently, multi-factor authentications have become more popular methods to achieve different levels of security than multi-password-composition polices.

High Burden leads to Bad Practice: Furthermore, Adams and Sasse [1] find that stringent password composition requirements significantly boost users' frustration and lead them to write down their passwords. They find that users are in general concerned to maintain security. However, they conclude existing security policies are not flexible to match users capabilities. As a result, these password policies can place burdens on users' side, and can lower the overall security by writing down or reusing their passwords. Also, Hanesamgar, et al.[7], also independently confirm the similar conclusion by performing the quantitative and qualitative analysis using users' real online accounts and their passwords. They show and validate that asking users to create a unique password for each account is not a good and realistic practice. One possible way to reduce users' burden is to use a password manager, which can manage and store users' passwords/credential. With a password manager, users do not have to worry about different password policies, as generally users only need to remember their master password to interact with a password manager. However, password managers have not been widely adopted, yet.

Weak and Not Usable: Complex password policy appears to increase password stronger. However, due to the recent advancement in password cracking methods[5], passwords with complex classes (3 or more classes) with 8 characters can be easily breakable using statistical guessing[8] or neural network-based method[5]. For example, "Password123" satisfies the 3class8 requirement, but it is easily crakable. Therefore, unfortunately complex password policies do not always guarantee strong password strength today. Shay et. al. [9] compared eight different password composition policies and found that a long password with fewer constraints can be more usable and stronger than a short passwords with more constraints, which may also lead to unsafe practices like writing down passwords [10]. Hence, we observe that complex password policies no longer correlate to higher security. Futhermore, usability the

complex policies provide is even worse.

Ⅲ. Approaches to Improve Current Password Composition Policies

Leveraging Blacklisted Passwords: Due to these serious problems with current password policies, NIST [6] in 2017 released the recommended guideline for a new textual password composition policy (NIST Special Publication 800-63B). The new guideline removes requirements for different character classes but keeps the length requirement. By removing complex class requirements, it is expected that users can create new passwords more easily with more flexibility.

Also, the system is required to check users' passwords with any previously leaked password or a password that contains common dictionary words (blacklisted passwords) as weak. The new guideline requires password system administrators to perform more extensive password checking than users do. Hence, the NIST guideline addresses some of users' frustrations by shifting more responsibility to systems. However, Habib et al.[4] conducted a large scale user study to analyze users' password creation behavior in the presence of blacklisted passwords. They analyzed 2,280 passwords from their user study, and found that participants who initially tried to use a blacklisted password ultimately created passwords with fewer characters, capital letters, digits, and symbols. In addition, those who reused a blacklisted password in their final password created passwords that were significantly easier to guess. Although more research is required, it appears to be still challenging that the new guideline cannot completely remove the problem of password reuse of a user with blacklisted passwords.

In addition, blacklist check is a simple string matching. Hence, it is very easy to bypass the check with slight modifications from the existing blacklisted passwords. Effectively, measuring and detecting similarity between users entered passwords and blacklisted passwords, and how to implement this are still open-questions.

Password Meters with Feedback: Another way to improve user's password choice is to offer real-time feedback on this choice and, optionally, suggestions for improvements. Password meters offer real-time feedback on user password strength [11, 12]. Although these feedback may be inconsistent as shown by many researchers[2, 13, 14], Ur et. al [5] presents the novel password strength design to improve users' password choices with proactive text feedback. Their data-driven password meter provides the accurate strength measure and detailed actionable feedback to users, showing a great promise. However, their evaluation conditions enforce different password composition policies at the same time with their password meters with feedback. For example, they found that their feedback did not improve password strength of users with a 3class12 policy. Therefore, it is unclear whether a password meter helps or the combined password meter with a password policy improves strength. The interplay between password composition policies and password meter with feedback needs to be better understood.

Ⅳ. Discussions

Existing password composition policies have several shortfalls today. They are not helping users to create strong passwords, and sometimes passwords produced under complex password policies are not usable. In order to address these issues, there is an on-going effort to improve password strength using blacklisted passwords. Also, password meters with textual feedback performed better than other prior approaches. However, more research is still needed in this area, as their benefits are not clearly understood with these approaches. Also, the system overheads, such as implementation, deployment cost, and complexity that system administrators have to face,

are not considered. For example, how frequently does a system need to update a blacklist, and what is a size of blacklist (used for a password meter) and how do we share them? In order to enable a wider adoption of new approaches, these factors must be addressed.

Ⅴ. Conclusion

In this paper, we focus on investigating the problems with existing password composition policies, and introduce two latest work in this area to improve password strength. However, still more research is needed to better understand the benefits of the proposed approach, considering usability as well as practical and deployment issues.

References

[1] Inglesant, Philip G., and M. Angela Sasse. "The true cost of unusable password policies: password use in the wild." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2010.

[2] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman. Of passwords and people: measuring the effect of password-composition policies. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pages 2595–2604. ACM, 2011.

[3] Ur, Blase, et al. "I added '!'at the end to make it secure": Observing password creation in the lab." Proc. SOUPS. 2015.

[4] H. Habib, J. Colnago, W. Melicher, B. Ur, S. Segreti, L. Bauer, N. Christin, and L. Cranor. Password creation in the presence of blacklists. 2017.

[5] B. Ur, F. Alfieri, M. Aung, L. Bauer, N. Christin, J. Colnago, L. Cranor, H. Dixon, P. E. Naeini, H. Habib, N. Johnson, and W. Melicher. Design and evaluation of a data-driven password meter. In CHI'17: 35th Annual ACM Conference on Human Factors in Computing Systems, May 2017.

[6] P. A. Grassi, J. L. Fenton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr, J. P. Richer, N. B. Lefkovitz, J. M. Danker, Y. Choong, et al. Draft nist special publication 800 63b digital identity guidelines. 2017.

[7] Ameya Hanesamgar, Simon S. Woo, Chris Kanich, and Jelena Mirkovic, "Leveraging Semantic Transformation to Investigate Password Habits and Their Causes", ACM SIG CHI2018 (to appear)

[8] M. Dell'Amico and M. Filippone. Monte Carlo Strength Evaluation: Fast and Reliable Password Checking. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pages 158–169. ACM, 2015.

[9] R. Shay, S. Komanduri, A. L. Durity, P. S. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer, N. Christin, and L. F. Cranor. Can long passwords be secure and usable? In Proceedings of the 32nd annual ACM conference on Human factors in computing systems, pages 2927–2936. ACM, 2014.

[10] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor. Encountering stronger password requirements: user attitudes and behaviors. In Proceedings of the Sixth Symposium on Usable Privacy and Security, page 2. ACM, 2010.

[11] S. Ji, S. Yang, T. Wang, C. Liu, W.-H. Lee, and R. Beyah. Pars: A uniform and open-source password analysis and research system. In Proceedings of the 31st Annual Computer Security Applications Conference, pages 321–330. ACM, 2015.

[12] D. L. Wheeler. zxcvbn: Low-budget password strength estimation. In Proc. USENIX Security, 2016.

[13] S. Egelman, A. Sotirakopoulos, I. Muslukhov,

K. Beznosov, and C. Herley. Does my password go up to eleven?: the impact of password meters on password selection. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pages 2379–2388. ACM, 2013.

[14] S. Ji, S. Yang, T. Wang, C. Liu, W.-H. Lee, and R. Beyah. Pars: A uniform and open-source password analysis and research system. In Proceedings of the 31st Annual Computer Security Applications Conference, pages 321–330. ACM, 2015.

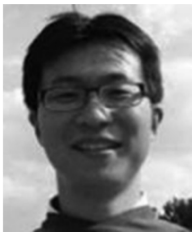
〈저 자 소 개〉

우 사이먼 (Woo. Simon)
정회원

2003년 : BSEE, University of Washington, Seattle, USA
2005년 : MSECE, University of California, San Diego, La Jolla, USA
2017년 : Ph.D. in CS, University of Southern California, Los angeles, USA
2017년～현재 : 한국뉴욕주립대학교 (SUNY, Korea) 컴퓨터과학과 조교수
관심분야 : 통신공학, 정보보호

정 경 주 (Kyeong Joo Jung)

Feb. 2017 : Bachelor of Computer Engineering, Yonsei University
Mar. 2017～current : Master program of Computer Science, Stonybrook University, SUNY Korea
Interest area : Information security, network security, usable security



최 봉 준 (Bong Jun Choi)

B.Sc of electrical and electronics engineering degrees from Yonsei University.
M.Sc. of electrical and electronics engineering degrees from Yonsei University
Ph.D. degree from the University of Waterloo in electrical and computer engineering
2011~current : Member, IEEE Communication Society
2011~current : Member, IEEE
2012~current : Member, ACM
2012～Current : Master program of Computer Science, Stonybrook University, SUNY Korea
Interest area : Energy Efficient Networks, Distributed Computing, Mobile Wireless Communications and Network, Network Security, and Smart Grid.