Personalizing Password Policies and Strength Feedback

Tobias Seitz

Ludwig-Maximilians-Universität München, Munich, Germany
tobias.seitz@ifi.lmu.de

Abstract. To make users pick stronger passwords, service providers utilize password policies and password creation feedback while the user types inside password fields. Those two techniques often fail to achieve this primary goal. In this position paper, we argue that a personalized version of polices and strength meters are worth investigating. Putting individuals into the center of attention rather than the tasks may improve the user experience of password-based authentication. We discuss the challenges and opportunities, and we outline how policies and password feedback can be tailored to specific users.

Keywords: usable security; authentication, passwords; personality

1 Introduction

Although the death of passwords has been announced many times[1], there is no clear roadmap to eliminate knowledge based authentication mechanism on the web: Passwords will be part of users' lives in the foreseeable future due to the lack of perfect alternatives. Since passwords bring numerous usability pitfalls, research in the domain of usable security has identified many aspects in users' attitudes and behaviors towards passwords. For instance, we know that users often choose weak passwords and re-use them across multiple websites [5]. This boosts the usability, but lowers security because it becomes simple for attackers to take control over weakly protected online profiles.

To make users pick stronger passwords, websites often ask users to include digits, symbols, or other characteristics in their secrets. There is a wide range of such password composition policies and many of them fail to achieve their goal of stronger passwords [12]. Some users try to get away with the simplest password that fulfills the requirements [8]. Other users are very careful in following the rules and even go beyond the requirements [13]. Current password policies do not account for these different user personalities. A website's password policy is the same for all users. However, such one-

[1] For instance, https://www.infosecurity-magazine.com/webinars/death-of-passwords/, http://www.gigya.com/resource/whitepaper/death-of-the-password/, https://www.cnet.com/news/gates-predicts-death-of-the-password/

In: R. Orji, M. Reisinger, M. Busch, A. Dijkstra, M. Kaptein, E. Mattheiss (eds.): Proceedings of the Personalization in Persuasive Technology Workshop, Persuasive Technology 2017, Amsterdam, The Netherlands, 04-04-2017, published at http://ceur-ws.org

fits-all approaches may not be the best solution to achieve better usability and security for individuals. We argue that a policy that respects the user's attitude towards password creation can be of merit for both users and the overall security of a service.

Besides enforcing password characteristics, there is also a softer approach in the form of persuasive feedback and password creation guidance. Most commonly, we encounter this type of interface design with password meters that rate the strength of a user's password as they type it. The effectiveness of password meters is well debated. For high-value accounts, Egelman et al. [4] found that such feedback can slightly boost password strength. Additionally, they found that for lower value accounts, adding a password meter is without noteworthy effects, but they do not seem to harm the experience. Yet, here again, users face a one-fits-all solution, because the password meter is the same for all users.

2 Opportunities Arising from Related Work

We build our argument at the intersection between usable security and persuasive technology. Persuading users and supporting behavior change regarding passwords was proposed in 2001 by Weirich and Sasse [16]. Since then, much work has focused on trying to nudge users to alter their behavior, but only seldom do we encounter the concepts and proposals in day-to-day web browsing. The most prevalent examples are password meters and real time feedback, i.e. a list of requirements that is checked off during password entry. These mechanisms have been studied extensively ([2, 4, 13, 15]). The bottom line is that users welcome real-time feedback, but strength meters have a limited effect on password choice.

A study by Ur et al. showed that users actually might not need such external feedback to judge the strength of a password correctly [14]. They found that users rated the strength of passwords fairly accurately, but also that many study participants were misled by characteristics like digits and common substitutions. This kind of misjudgment and subpar strength feedback call for novel ideas.

To approach this opportunity, a recent large scale survey suggests that there are two common types of user personalities regarding passwords [9]: "Type A" users that have a strong urge to stay in control of their digital footprint and "Type B" users that convince themselves that their data is not valuable for attackers. The study finds that both types of users do not believe to be at risk. The data can be seen as further evidence that the risk of being attacked strongly depends on the user personality, as was already suggested earlier [7, 16, 19]. Consequently, it is time to follow the proposal from the persuasive authentication framework (PAF) to consider personalization as persuasion principle [6]. Forget et al. argue that a personalized system can help improve the users' mental model of security.

To the best of our knowledge, such personalized systems do not exist. We propose to respect the user's personality in the way password policies enforce and communicate requirements. Ultimately, this is an opportunity make such mitigations more effective in terms of supporting the user in picking an adequate secret.

3 Critical Challenges

There are a couple of major challenges of personalizing password policies and strength feedback. First, before we can adapt user interfaces to individuals, an in-depth assessment of their personality is required. There are a variety of widely approved personality tests, e.g. the NEO-PI-R [1], but they all expect active user involvement. Demanding this kind of action seems unrealistic. Thus, an implicit assessment is mandatory, which is already possible with an analysis of mobile phone usage data [18] or digital footprints [3]. These current solutions are privacy invasive, so we need to adjust them to achieve a more ethically reasonable level. Users may also want to fine-tune automatic assessments, so the system needs to provide such means. Also, personality assessments could be inaccurate, so users need to be able to reset the assessment.

Second, when a user picks a password, a website does not have any information about him or her, other than the manually provided user name, password, and perhaps bits of personal information. If we aim to personalize this dialog between website and user, there needs to be a way to exchange a personality profile between the two parties in an unobtrusive, privacy-sensitive manner. To make sure the users stay in control of their information the protocol needs to ask permission or at least read general settings about with whom to share personality profiles. Intensive work is going to be needed to carefully design systems that respect user preferences and eventually achieve broad acceptance.

4 Research Agenda

The challenges and opportunities deliver an actionable research agenda, which we briefly illustrate with potential use cases and scenarios. Most of them require a modification of web browsers, or capabilities that can already be added with browser extensions.

4.1 Personalized Password Policies

Currently, password policies enforce the same rules on all users, i.e. length and complexity requirements. Still, there are different policies that deliver similarly strong passwords [12]. As outlined above, we envision a new paradigm that modifies these rules depending on the user's personality characteristics. Such a personality profile can consist of a score on each of the five dimensions of the Big-Five model [1] to be minimally privacy invasive. When the website recognizes a new user who scores high on openness, it can switch to a policy that focuses on password length rather than complexity classes, because these individuals are often very creative and constraints might be counterproductive [10]. On the contrary, policies can make highly conscientious people add various character-classes. It is likely that these users will benefit from an explicit list of requirements when they have to come up with a strong password, which can be diligently checked off requirement by requirement. Ideally, such a dynamic personalized policy would reduce the burden on users while achieving the same level of security.

4.2 Tailored Password Nudges

So far, nudging during password selection is mostly done with password meters or concrete suggestions. The Safari browser automatically pops-up password suggestions when users register on new web sites. In our past work, we have studied the influence of different password suggestions on self-selected passwords [11]. The suggestions were rejected by most participants, but the strength of self-selected passwords significantly increased upon seeing a password suggestion. We believe that we can design such mechanisms around personality traits to make password suggestions more effective. Suggestions should therefore respect user preferences to become more powerful. For instance, Safari could try different variations of password topologies to find out which passwords are most attractive to the user and on which web sites. Additional information on the user's personality might help but is not mandatory in this scenario. Again, such a personalized system can boost usability while adding to the overall security. However, we have to ensure that attackers do not benefit from personality models, which is a critical challenge.

4.3 Feedback Based on Re-Use Patterns

Finally, to better cope with authentication overhead, users re-use their passwords many times [5]. We could use this kind of behavior to create prediction models for future registrations. The models might predict which password is going to be used on the web page for which the user creates an account. In this opportune moment, a personalized system can detect anomalies and intervene if another password from the portfolio might be a better fit for the website at hand. For instance, if a user tries to sign-up to PayPal using the same password as with their email account, the system can discourage this without blocking the action. Such an approach is designed around the individual user and their preferred re-use strategy. Infrequent suggestions like this could make better options more salient.

5 Conclusion

At the moment, the challenges to tailor security mitigations to specific users seem big. We do not know how users will react to such personalized systems in security contexts. However, since users will have to deal with passwords for the foreseeable future, we believe the challenges are worth taking and they can be approached in small steps. It will take careful design and long-term evaluation to have browser vendors consider implementing personalized security mitigations. The first small step is to mock-up the interaction and evaluate concepts in Wizard-of-Oz studies to obtain a better understanding of user reactions and attitudes towards personalized policies and feedback.

References

1. Costa, P.T., McCrae, R.R.: Revised NEO personality inventory (NEO PI-R) and NEO five factor inventory (NEO FFI): Professional manual. Psychological Assessment Resources 3, 101 (1992)
2. de Carné de Carnavalet, X., Mannan, M.: A Large-Scale Evaluation of High-Impact Password Strength Meters. ACM Transactions on Information and System Security 18(1), 1–31 (2015)
3. De Montjoye, Y.A., Quoidbach, J., Robic, F., Pentland, A.: Predicting personality using novel mobile phone-based metrics. Lecture Notes in Computer Science 7812 LNCS, 48–55 (2013)
4. Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K., Herley, C.: 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 (CHI '13). pp. 2379–2388 (2013)
5. Florêncio, D., Herley, C.: A Large-Scale Study of Web Password Habits. In: Proceedings of the 16th international conference on World Wide Web (WWW '07). pp. 657–665. ACM (2007)
6. Forget, A., Chiasson, S., Biddle, R.: Persuasion as Education for Computer Security. In: Proceedings of E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education. pp. 822–829. Association for the Advancement of Computing in Education (AACE), Chesapeake, VA (2007)
7. Herley, C., Pieters, W.: "If You Were Attacked, You'd Be Sorry": Counterfactuals as Security Arguments. Proceedings of the 2015 New Security Paradigms Workshop pp. 112–123 (2015)
8. Inglesant, P., Sasse, M.A.: The True Cost of Unusable Password Policies: Password Use in the Wild. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10). pp. 383–392 (2010)
9. LastPass: The Password Paradox and why our Personalities will get us Hacked. Tech. rep. (2016), http://prod.cdata.app.sprinklr.com/DAM/434/LastPass_ExecutiveSummary-44b1d9ef-209a-400a-865d-d0462920ca5b-1914739482.pdf
10. McCrae, R.R.: Creativity, divergent thinking, and openness to experience. Journal of Personality and Social Psychology 52(6), 1258–1265 (1987)
11. Seitz, T., von Zezschwitz, E., Meitner, S., Hussmann, H.: Influencing Self-Selected Passwords through Suggestions and the Decoy Effect. In: Proceedings of the 1st European Workshop on Usable Security. Internet Society, Darmstadt (2016)
12. Shay, R., Durity, A.L., Segreti, S.M., Ur, B., Bauer, L., Christin, N.: Designing Password Policies for Strength and Usability. ACM Transactions on Information and System Security 18(4), 13:1–13:34 (2016)
13. Shay, R., Ur, B., Bauer, L., Christin, N., Cranor, L.F., Forget, A., Komanduri, S., Mazurek, M.L., Melicher, W., Segreti, S.M.: A Spoonful of Sugar? The Impact of Guidance and Feedback on Password-Creation Behavior. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '15). pp. 2903–2912. ACM (2015)
14. Ur, B., Bees, J., Segreti, S.M., Bauer, L., Christin, N., Cranor, L.F.: Do Users' Perceptions of Password Security Match Reality? In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16). pp. 3748–3760. ACM (2016)
15. Ur, B., Kelley, P.G., Komanduri, S., Lee, J., Maass, M., Mazurek, M.L., Passaro, T., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L.F.: How Does Your Password Measure Up?

The Effect of Strength Meters on Password Creation. In: Security'12 Proceedings of the 21st USENIX conference on Security symposium. pp. 5–16 (2012)
16. Weirich, D., Sasse, M.A.: Pretty Good Persuasion: A First Step towards Effective Password
17. Security in the Real World. In: Proceedings of the 2001Workshop on New Security Paradigms (NSPW '01). pp. 137–143. ACM, New York, NY, USA (2001)
18. Youyou, W., Kosinski, M., Stillwell, D.: Computer-based personality judgments are more accurate than those made by humans. Proceedings of the National Academy of Sciences 112(4), 1036–1040 (2015)
19. Zakaria, N.H., Katuk, N.: Towards designing effective security messages: Persuasive password guidelines. In: Proceedings of the International Conference on Research and Innovation in Information Systems, ICRIIS. pp. 129–134. IEEE Computer Society (2013)

All links were last followed on February 09, 2017.