Improving the Design and Usability of Password Creation Systems

Saja Althubaiti
Human Computer Interaction Research Group
Department of Computer Science
University of York, York UK YO10 5GH
saaa505@york.ac.uk

CHI'17 Extended Abstracts, May 06-11, 2017, Denver, CO, USA
ACM 978-1-4503-4656-6/17/05.
http://dx.doi.org/10.1145/3027063.3027131

Abstract
The usability of Password Creation Systems (PCSs) as interactive systems has been neglected in research compared to work on developing individual features for creating passwords such as strength meters. PCSs can include a strength meter, statement of password policy, suggestions for creating good passwords and feedback to users about errors. If users are struggling to understand how the PCS works due to usability issues, they will have less cognitive effort available to put into creating a strong password. Studying the usability of PCSs and ensuring they support users well when creating passwords is therefore an important issue. A series of studies is being conducted to understand the problems users encounter with PCSs, develop a model of PCSs, understand how PCSs should organize their supporting features, and to propose a set of heuristics for use in guiding the development of PCSs and in expert evaluations.

Author Keywords
Passwords; Usability; Password policy; Strength indicators; Password creation suggestions; Authentication;

ACM Classification Keywords
D.4.6 Management Of Computing and Information Systems: Security and Protection—Authentication

Research Motivation and Background

Textual passwords are widely used although they continue to create many problems for users and major concerns for the online security community. Users create passwords using what can be considered small interactive systems consisting of one or more screens, which include messages, strength indicators and other elements. Such Password Creation Systems (PCSs) are a particular class of interactive system and as such present their own usability problems. Recent evidence has shown that users encounter numerous usability problems when creating passwords [6]. If users are struggling to understand how a PCS works, that will take away cognitive effort which could be used to create a strong and yet memorable password. Recent research has shown that cognitive effort is necessary for creating good passwords [5].

Most users seem burdened with many textual passwords which they need to remember and use in many different systems [4]. They often sacrifice security for convenience [8]. To remember passwords, users tend to choose an easy-to-remember but easy to crack strings of letters and numbers (and only occasionally other symbols). Many studies have shown that the weaknesses in passwords result primarily from users' behavior [e.g. 1,7]. Choosing a good password, which is both strong and memorable, is the first stage of this behavior chain. Therefore, studying the usability of PCSs and ensuring they support users well when creating passwords is important. Considerable attention has been given recently to providing users with support for creating passwords with particular features within PCSs such as password strength indicators [9]. However, apart from some preliminary work [2], we have not been able to find any research which has explored the usability of PCSs as whole interactive systems in their own right and the usability of the support which they provide to users in the creation of passwords. Although developers have implemented different support features for designing PCSs, users continue to choose weak passwords [3].

PCSs may have three supporting features that help users in choosing passwords: (1) password policy statements, (2) password creation suggestions and (3) password strength indicators. However, previous studies have focused on examining the security and memorability of chosen passwords rather than looking at how these features integrate into the user interface of the PCS and their effect on password choice. To my knowledge, none of the previous studies have looked at the design and implementation of these features at the user interface level or from the user perspective. Most of what is now available in PCSs is implemented in an ad hoc manner, rather than by examining users' needs (while always considering security issues); for instance, when do users want particular features to be presented, how do users want them to be presented. Current implementations of the supporting features are very varied and this may cause users' confusion as they move from one PCS to another. Furthermore, the guidance provided by existing systems often does not seem adequate for users when choosing a password. For example, some systems provide a password strength indicator but it provides no clues about how to increase password strength or why the currently chosen password is weak. My research focuses on how to resolve these issues.

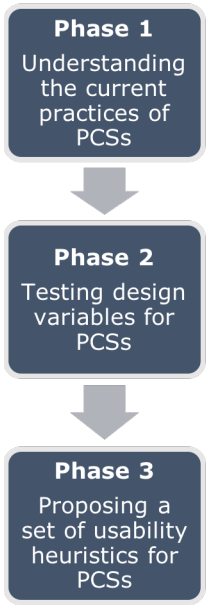

Figure 1: Three phases of this research programme

Research Questions and Aims

The central question of this research asks how can PCSs effectively support users in creating passwords without compromising security? This question will be addressed by breaking this research into three phases, as shown in Figure 1. The first phase focuses on understanding current practices in PCSs. It looks at the frequency and characteristics of the supporting features. Then, it investigates the usability problems which users encounter by conducting both user and expert evaluations of a number of PCSs. The second phase examines the effect of design aspects in PCSs. Each supporting feature is examined individually to explore effective ways of designing the particular feature. I then investigate whether the presence of a combination of more than one supporting features in a PCS influences the password creation process. Finally, the third phase will use the results from the previous two phases to develop and validate a set of usability heuristics specifically for the design and evaluation of PCSs.

Research Approach

To address the central research question, seven studies were planned. In phase one, three studies have been completed (see Figure 2). For phase two, three studies are in progress (see Figure 3). Finally, for phase three, the seventh study sums up the research programme. These studies are described briefly below, alongside the results of the completed studies.

Study 1: an analysis of current PCSs

This study gave an overview of current practices in PCSs and provided a better understanding of the password creation process. An analysis of 29 current PCSs was conducted, with PCSs being analyzed by the researcher and her supervisor. Many different passwords were tried on each PCS to elicit a wide range of behaviors and particularly errors. In particular, three features were examined: password policy, password creation suggestions and password strength indicators. This analysis led to a general model of PCSs.

Study 2 and Study 3: expert and user evaluation of current PCSs

These studies assessed the levels of usability of current PCSs with both expert and user evaluation. Six PCSs were chosen from the set analyzed in Study 1. An expert review method (n=7) and a concurrent think-aloud protocol (n=24) user evaluation were used. Results were compared to examine the types and numbers of usability problems that experts identify and users experience. The two evaluations produced a pool of 121 usability problems: 33.1% found by experts, 31.4% by users, and 35.5% by both experts and users. The results showed that many usability problems related to the lack of support features such as a policy statement, suggestions on how to make a good password or a strength indicator.

Study 4: instructions for creating passwords

This study aimed to find what forms of instructions users prefer for the presentation of password policies and password creation suggestions. In an online study, 117 respondents rated and commented on different possible instructions in the context of actually creating a password. The results indicated users prefer declarative statements of policy before and after they interact with the PCSs. However, they prefer procedural statements of policy during their interaction with PCSs. Regarding suggestion statements, users prefer declarative statements before and during their

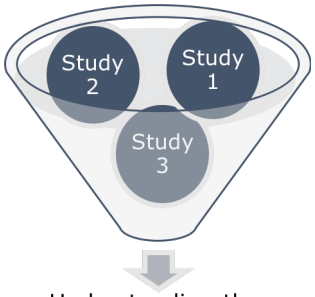

Figure 2: Studies of phase one

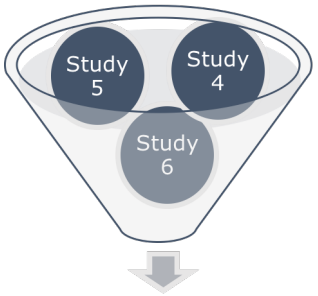

Figure 3: Studies of phase two

interaction, whereas, they prefer procedural statements after interaction.

Study 5: Presentation effects
This study will investigate the most effective point at which to present password policy and creation suggestions to users in a PCS, the most effective ways to present these features and the features for the most effective overall design for password strength indicators. An online study will involve two parts: participants will be asked to create a number of passwords using different supporting features. Three days later they will be asked to recall the created passwords.

Study 6: Combined effects
The study will examine the combined effect of presenting more than one supporting feature in a PCS, building on the results of Study 5.

Study 7: Usability heuristics and their validation
Upon completion of the two phases, this study will develop and validate a set of usability heuristics specifically for the design and evaluation of PCSs. Also, a comparative evaluation will be made to ensure the effectiveness of the new heuristics.

Contributions

The contributions of this research are : (1) understanding the problems which people encounter with creating passwords by collecting a corpus of usability problems with PCSs through user and expert evaluations; (2) understanding of how PCSs should organize their supporting features by conducting user studies which manipulate these features; and (3) proposing a set of heuristics for use in guiding the development and evaluation of PCSs.

References

1. Alan S Brown, Elisabeth Bracken, Sandy Zoccoli, and King Douglas. 2004. Generating and remembering passwords. *Applied Cognitive Psychology* 18, 6: 641–651.
2. Richard M Conlan and Peter Tarasewich. 2006. Improving interface designs to help users choose better passwords. In *CHI '06 extended abstracts on Human factors in computing systems - CHI EA '06*, 652.
3. Dinei Florencio and Cormac Herley. 2007. A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web - WWW '07*, 657.
4. Beate Grawemeyer and Hilary Johnson. 2011. Using and managing multiple passwords: A week to a view. *Interacting with computers* 23, 3: 256–267.
5. Thomas Groß, Kovila P L Coopamootoo, and Amina Al-Jabri. 2016. Effect of Cognitive Effort on Password Choice. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*.
6. Helen Petrie and Christopher Power. 2012. What do users really care about?: a comparison of usability problems found by users and experts on highly interactive websites. In *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems*, 2107–2116.
7. Martina Angela Sasse, Sacha Brostoff, and Dirk Weirich. 2001. Transforming the "weakest link"—a human/computer interaction approach to usable and effective security. *BT technology journal* 19: 122–131.
8. L Tam, M Glassman, and M Vandenwauver. 2010. The psychology of password management: a tradeoff between security and convenience. *Behaviour& Information Technology* 29, 3: 233–244.
9. Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, and Lujo Bauer. 2012. How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. In *USENIX Security Symposium*, 65–80.