International Journal of Technology and Human Interaction
Volume 17 • Issue 1 • January-March 2021

The Impact of Keyboard Type on Users' Perceptions of Password Strength

Philip Kortum, Rice University, USA
Claudia Ziegler Acemyan, Rice University, USA

ABSTRACT

With the proliferation of mobile touchscreen computers, password entry no longer takes place exclusively on physical keyboards. Entering a strong password on a mobile device requires a person to navigate through multiple keyboard depths to access each character, while entering the same password on a desktop keyboard only requires a user to press keys that are accessible on a single layer. This paper investigates whether the extra physical and cognitive effort associated with using multiple levels of onscreen keyboards changes users' perceptions of password strength. Sixty participants judged perceived security by typing 36 passwords with a differing number of keyboard level transitions on either a mobile device or a desktop keyboard. Analysis revealed that passwords requiring a user to transition between keyboards increased perceptions of security. Passwords that required the use of the shift key on a desktop keyboard returned similar results. This suggests that users may overestimate the security of passwords based on the number of entry keystrokes.

KEYWORDS

Entropy, Keyboards, Mobile Computers, Mobile Devices, Security, Security Perception, Soft Keyboards, Usability

INTRODUCTION

Passwords are one of the first lines of defense that users employ to access secure computer systems and protect personal information (Furnell & Zekri, 2006), and are likely to remain as a primary security mechanism for the foreseeable future (Bonneau, Herley, Van Oorschot, & Stajano, 2012; Bonneau & Preibusch, 2010; Herley & Van Oorschot, 2012; Siddique, Akhtar, & Kim, 2017). Even though passwords have been used for over four decades, users still often create and use weak passwords (Taneski, Hericko, & Brumen, 2014) and tend to reuse them across sites (Das et al 2014; Wash, Rader, Berman, & Wellmer, 2016), as they are often easier to generate and remember this way. However, the recent reoccurrence of high-profile data breaches (e.g. Cooper, 2015; Gressin, 2018; Maltis, 2016; McMillan, 2016) has focused the public's attention on the importance of password security and the need to create harder to crack passwords. These data breaches might also be responsible for changes in human behavior, like the recent observed trend of users strengthening their passwords (Shen, Yu, Xu, Yang & Guan, 2016), although some researchers have suggested that while these attacks get the

DOI: 10.4018/IJTHI.2021010106

attention of users, they do not impact their behaviors in password creation or management (Curtis, Carre & Jones, 2018).

Although there is evidence that users can determine if a password is 'good' or not (Tam, Glassman & Vandenwauver, 2010; Seitz & Hussmann, 2017), the *actual* security of passwords often does not match users' *perceptions* of password security (Ur et al 2016). Further, different people may have different perceptions of password security based on prior knowledge or personal characteristics (Butler & Butler, 2018; Cordova, Easton, Greer & Smith, 2018). System administrators may try to help users create secure passwords by implementing strong password creation policies, criteria, or training (Furnell, & Esmael, 2017; Komanduri et al, 2017; Mwagwabi, McGill, & Dixon, 2014), but even when users know what constitutes a good password, the ways in which they implement that knowledge in the real world is predictable, making the resulting passwords less secure (Dell'Amico, Michiardi, & Roudier, 2010; Shay et al 2014)

Importantly, there is considerable disagreement among computer security specialists about strong password criteria and how to measure password security (Castelluccia, Dürmuth, & Perito, 2012; Kelly et al, 2012; Ma, Campbell, Tran & Kleeman, 2010). Consequently, when these experts develop different password strength checkers, there are disparate results (de Carné de Carnavalet & Mannan, 2014; Ji et al, 2017).

It is easy to see how this situation could lead to significant confusion for users when they try to create the strongest passwords possible. Under these kinds of conditions, it is not unreasonable to assume that users may be creating their own set of heuristics about what constitutes a strong password based on their synthesis of all information currently available, both formally and informally. Yet, given the role that people play in the creation of passwords, there is surprisingly little research describing how those users perceive the security of their passwords.

Humans are integral to the password security process (Furnell & Clarke, 2012). A person has to create a password that meets or exceeds the criteria set by system administrators, remember the password, and then be able to recall and input the password on demand. Because users generally try to minimize the cognitive demands of any task (Payne, Bettman, & Johnson, 1993), there is always a tension between creating a password that is easy to remember (e.g., a short, simple word) and a password that is stronger (e.g., one that is long, excludes words, randomly generated, and includes both special characters and upper and lowercase characters).

There is a robust body of research on the usability of passwords and the need for passwords to be usable (Adams, Sasse, & Lunt, 1997; Schultz, Proctor, Lien, & Salvendy, 2001; Stanton & Greene, 2014; Vu et al, 2007; Yan, Blackwell, Anderson, & Grant, 2004), and the interplay between usability and security is a long-recognized problem (Klein, 1990; Morris, & Thompson, 1979; Zviran, & Haga, 1999). If passwords are too hard to remember and/or input into a system, users will invariably find ways to make using them easier. Walk around an office where there is a strict password security policy in place that requires frequent password changes, while also prohibiting the use of previously used passwords, and one is likely to observe passwords written on sticky notes stuck to monitors (Stanton, Stam, Mastrangelo, & Jolton, 2005)—a practice that ultimately circumvents security measures. This does not happen because users want their systems to be insecure. Rather, users understand that computer security is important (Albrechtsen, 2007; Lightner, 2003), but the security procedures likely place too great of a cognitive burden on users, causing them to adapt by taking shortcuts.

Users might also lack knowledge about how to adequately protect their computers (Adams & Sasse, 1999) or lack the desire to do so (Hart, 2008)—further impacting their decisions and behavior in ways that result in reduced system security thorough password reuse (Ives, Walsh & Schneider, 2004), the selection of weak passwords even though they "know better" (Shay et al, 2010; Riley, 2006), or other maladaptive behaviors such as recording every user name and password in an unencrypted file in an easily accessible location. These behaviors occur because the password requirements push