One Size does not Fit Mobile: Designing Usable Security Input on Mobile Devices

Ann-Marie Horcher, Ph. D.

Central Michigan University
horch1a@cmich.edu

ABSTRACT

Text entry of strong passwords on the virtual keyboard of a mobile device demands more cognitive effort than is safe at any speed. Users are walking into traffic, veering off the beaten path, and colliding with lampposts while using virtual keyboards. Virtual keyboards on mobile devices have been designed to fit smaller screens by shrinking the size of the keys. To compensate for the inevitable keying errors caused by the difficulty of acquiring the desired key target, virtual keyboard software relies heavily on predicting input. While this anticipation works reasonably well for text messages and input based on the correct spelling of words of the language in use, it does not improve the accuracy of security input.

Security input is the entry of character strings to achieve authentication. Security input exhibits atypical patterns due to strong password rules. Strong passwords require key sequences with special characters and numerals that are less common in normal text input. Virtual keyboards reflect this reality by making these characters less convenient to type and/or hard to locate. To protect against password detection via shoulder-surfing, security input is not displayed. The user receives zero visual feedback on the accuracy of the input.

To achieve usability in security interface navigation on mobile devices for basic authentication, the virtual keyboard for security input needs to be optimized for security input in layout, size, and anticipatory behavior. In this research a virtual keyboard designed to meet human interface guidelines for small touchscreens and to follow known usability design principles is used to mimic basic authentication with strong passwords on mobile devices. The usability of the revised virtual keyboard is measured for efficiency, effectiveness, and user satisfaction.

1. INTRODUCTION

Human error is a significant, poorly recognized, but enduring issue in information systems security [4, 20]. Usable design reduces human error [28], and is critical to effective security [9]. Security design on mobile devices presents challenges due to the constraints of the device [33], and opportunities based on the enhanced capabilities. Authentication by fingerprint [29], touch patterns on the screen [27], and facial recognition [47] are all options that do not rely upon text entry for primary authentication. Graphical passwords which involve recognition instead of input have also been explored on mobile [7, 13, 40].

USENIX Symposium on Usable Privacy and Security (SOUPS) 2018. August 12 -- 14, 2018, Baltimore, MD, USA.

Basic authentication, or the entry of a user identifier and password [8], relies on text entry. In spite of the non-text entry options for mobile platform, basic authentication is still the most prevalent and used as an alternate, backup, or recovery method to non-text authentication [19]. Basic authentication, in spite of its weaknesses, is still the ISO standard for entity authentication [3].

Basic authentication was designed in a desktop setup, where text is entered efficiently and comfortably using a physical keyboard [37]. To accommodate text entry needs on the small touchscreen typical of mobile devices, the miniaturized keyboard was adopted [46]. The virtual keyboard common on mobile devices does not provide the same comfort or efficiency as the physical equivalent [24]. Predictive text algorithms counteract the human error inherent in keying accuracy and the difficulty in acquiring targets smaller than 44mm square [12]. These algorithms depend on grammar and context [44]. Passwords that follow strong password guidelines [18] should not trigger or benefit from predictive text algorithms to prevent hacking.

The Common Industry Format (CIF) for usability testing uses the ISO 9241-11 definition of usability which is how well a product used by specified users achieves specified goals for effectiveness, efficiency, and user satisfaction [23]. The study findings from Kim et al. [25] indicate that virtual keyboards with a key size less than 16 mm may be too small for touch typing. With the small target the virtual keyboards do not meet the criterion for effectiveness in hitting the desired key accurately. Typing speed on virtual keyboards is 60% slower than desktop or notebook, so virtual keyboards in general also do not meet the criterion for efficiency [24]. Finally the continued research in virtual keyboard optimization on mobile devices shows user satisfaction is not achieved [2].

Ignoring the non-predictive nature of security input has resulted in a lack of usability that drives users to choose less secure passwords to be able to easily type them on mobile [30]. Humans choose to get the job done [43]. They resort to security input practices that may satisfy automated password strength meters, but violate the intent of the restrictions to achieve sufficient usability. This research examines whether applying known usability design principles to text entry of security input will result in a higher degree of usability.

2. BACKGROUND

Apple's iPhone Human Interface Guidelines recommend a minimum target size of 44 pixels wide 44 pixels tall, and Microsoft's Windows Phone UI Design and Interaction Guide suggests a touch target size of 34px with a minimum touch target size of 26px. Nokia's

developer guidelines weigh in on the low side suggest that the target size should be no smaller than 1cm x 1cm square or 28 x 28 pixels [1]. Android guidelines are the most generous at 48 pixels square [16]. The standard miniaturized virtual keyboards for smartphones on each these platforms all have keys smaller than these guidelines.

Approaches to solving the too small keyboard target involve making the keyboard bigger [34] and predicting the text input to compensate for keying error [11, 26, 38, 44]. Selective zooming to make portions of the keyboard bigger has been used to make the target temporarily bigger [34]. The frequency of usage of icons was used to predict which icons should be bigger, combining enlargement with prediction [22]. Enlargement of the keys based on which word the user might be typing has been studied with little accuracy gain, but greater user satisfactions [15].

Even though turning the smartphone to landscape mode automatically enlarges the keyboard, users much prefer portrait mode for stability [41]. One-handed text input is popular, typically using the thumb [35, 36]. Touch typing of security input on mobile is significantly more difficult due to both target size and the special characters required for strong passwords [30].

Security input that follows password strength rules uses character sequences with upper and lower case characters, numbers, and special characters [18]. Strong passwords are also misspelled, and not dictionary words. QWERTY layout gives keying advantage to the touch typist for alphanumeric input, but not for special characters [14]. A multi-touch interface to interact with special characters requires additional gesture recognition software, and a high level of complexity.

The gap in the literature that this study addresses is studying usability of security input on mobile devices that also includes the special characters required for password strength. If alphanumeric and special character input are equally usable on the mobile platform, users would not avoid broadening the character content of passwords because the character sequence are too time-consuming and difficult to type on mobile.

The hypotheses in the study mirror those used in earlier study on measuring the usability of virtual keyboards by Schaub et al. at Ulm University [39]. This study also concluded that low usability virtual keyboards were more resistant to shoulder-surfing due to the small button size.

The keyboard design insights of this study suggested that special characters should be made more accessible. A second recommendation was to avoid magnification of password input to obscure the text from observers. The study did not consider the alternative of a separate security input optimized keyboard, but provided recommendations based on the assumption of a single keyboard. The results of the Schaub study are used as a baseline for the measurement of the optimized security input keyboard.

3. Study Design

To assess the usability of virtual keyboard optimized for security input, this study collects a measure for each dimension of usability as defined by ISO [21]. The efficiency of the optimized keyboard is measured by the accuracy of the security input. The effectiveness of the optimized keyboard is measured by speed of the entry of the security input. Finally user satisfaction is measured by the Standardized Usability Scale (SUS). Therefore the study has the following hypotheses.

H1 Significant differences exist in the accuracy of security input on the optimized virtual keyboard.

H2 Significant differences exist in the speed of security input on the optimized virtual keyboard.

H3 Significant differences exist in the user satisfaction with security input on the optimized virtual keyboard. .

The methodology used was design science research (DSR). Design research (DR) is research into or about design. DSR is research using design as a research method or technique [17]. DSR methodology has a series of steps that result in specific outputs. It can be an iterative process, as information from an evaluation influences the design of another element [45]. Based on the feedback from the initial stages, the design is iteratively adjusted and improved.

A web application was created as the artifact to collect the data. The following requirements were observed.

1. All the screen targets need to be 44 or more pixels square to meet human interface design guidelines.
2. The screen needed to present on a single screen for most current models of smartphone
3. Special characters and numbers needed to be as easy to type as alphabetic characters
4. The user cannot see the input, to replicate the security input experience typical in the field
5. The user should receive clear feedback on input success, accuracy, and speed.

The study began with an entry questionnaire to be filled out on a mobile device. The input targets in the questionnaire were also designed to meet human interface design guidelines also used in the keyboard. The questionnaire was reached through a mobile-optimized website that explained the goal of the study. Participants were assured no personal passwords should be used and all security input measured in the study would be provided.

The questionnaire gathered demographic information (age, gender, technology expertise) and asked participants to specify brand and model of their primary mobile phone. The questionnaire reminds the participant to use their prescription glasses, if required.

The first version of the security-optimized keyboard appears full-sized in Figure 1. It uses keyboard layout uses an alphabetic order instead of QWERTY layout. The QWERTY layout has been very successful for traditional text entry [5]. The value of the touch-typing interface is suspect for security input, particularly for stronger passwords [30]. Strong passwords should not contain only dictionary words to avoid brute force cracking [6]. The three random word password advice given previously [10] has been proven unwise based on the strength of current password crackers [31]. Using a keyboard that does not favor touch-typing for security input will hopefully demotivate the inclusion of words in passwords.

The special characters and numbers are also placed at the top of the screen to make them "easy" to type. The special characters don't have the same consistency in keyboard placement on virtual keyboards as the alphabetic characters. The first row contains the most frequently used characters, then the punctuation marks, and finally mathematical symbols.

Users are also offered the option in the keyboard to switch the default layout of the alphabetic characters to QWERTY. This feature implements the usability principle proposed by Shneiderman et al [42] that puts the user in control.

.

Figure 1 Security-optimized virtual keyboard for mobile

4. Subjects and Procedure

The pilot group of subjects was 8 students in an online security class. The group ranges from 20-50 years in age, and is evenly split between the genders. The small group of subject is typical for usability studies., due to research which shows five subjects will identify 85% of the design problems in an interface [32].

For four weeks the subjects receive a text message with a link to the version of the webapp for the week. In the webapp they are challenged to type a series of strong passwords provided to them. At the end the user answers the SUS survey for that variation of the keyboard. The password input used in the study duplicated the password sequences used in the Schaub study [39]. Additional sequences were added to explore the usability of special characters which were omitted in the previous study. Strong password guidelines [18] have evolved to make special characters a common requirement. The results of the Schaub study are used as a baseline measurement of the optimized security input keyboard for shared password sequences.

5. Preliminary Results and Discussion

Though third party keyboards are disabled for security input through the primary OS for applications, the keyboard on input fields for web pages depends on proper HTML5 tagging. The same behavior as the default security behavior can also be created though coding.

The current version of the keyboard does not use an algorithm to check for the presence of a strong password. However, applying such a feature would allow prediction of what characters a user should need to type next. For example, if a user was inputting a strong password, and certain requirements had not been met, those portions of the keyboard that input that data could increase in size, or move to the top.

Changing the mobile keyboard changes the usability of security input. Currently mobile users avoid passwords that are difficult to type on the keyboards due to position, number of extra keys. The increased usability of larger character set should make more complex passwords easier to type.

A different keyboard may be seen as a violation of the consistency design principle [42]. There is already precedence in this for variable keyboards being presented based on HTML5. An email tag on an input field will produce a keyboard with the "@" sign next to the space bar.

The ABC layout vs. QWERTY is non-consistent in default keyboard presentation. Precedence for this is also shown through the use of a numbers only keyboard for the input of passcodes and phone numbers. These numbers only keyboards do present touchscreen targets that are obeying the 44mm size guideline and not utilizing predictive text.

Though preliminary numbers are still being generated, improvement of usability is highly likely. The usability of current mobile keyboards fails all three ISO criteria: efficiency, effectiveness, and user satisfaction. The keyboards using more screen real estate received immediate positive feedback.

6. REFERENCES

[1] Anthony. "Finger-Friendly Design: Ideal Mobile Touchscreen Target Sizes," May 5, 2018; https://www.smashingmagazine.com/2012/02/finger-friendly-design-ideal-mobile-touchscreen-target-sizes/.

[2] Armstrong, P., and Wilkinson, B., "Text entry of physical and virtual keyboards on tablets and the user perception," *Proceedings of the 28th Australian Conference on Computer-Human Interaction*, pp. 401-405, 2016.

[3] Basin, D., Cremers, C., and Meier, S., "Provably repairing the ISO/IEC 9798 standard for entity

authentication," *Proceedings of the First international conference on Principles of Security and Trust*, pp. 129-148, 2012.

[4] Baskerville, R., "Information systems security design methods: implications for information systems development," *ACM Comput. Surv.,* vol. 25, no. 4, pp. 375-414, 1993.

[5] Bi, X., Smith, B. A., and Zhai, S., "Quasi-qwerty soft keyboard optimization," pp. 283–286, 2010, 2010.

[6] Bonneau, J., and Shutova, E., "Linguistic properties of multi-word passphrases," *International Conference on Financial Cryptography and Data Security*, pp. 1-12, 2012.

[7] Chiang, H.-Y., and Chiasson, S., "Improving user authentication on mobile devices: a touchscreen graphical password," *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*, pp. 251-260, 2013.

[8] Chiasson, S., Forget, A., Stobert, E., Oorschot, P. C. v., and Biddle, R., "Multiple password interference in text passwords and click-based graphical passwords," *Proceedings of the 16th ACM conference on Computer and communications security* pp. 500-511, 2009.

[9] Cranor, L. F., and Garfinkel, S. L., *Security and Usability: Designing Secure Systems that People Can Use*: O'Reilly and Assoc., 2005.

[10] Dhillon, G., and Moores, S., "Computer crimes: theorizing about the enemy within," *Computers & Security,* vol. 20, no. 8, pp. 715-723, 2001.

[11] Dunlop, M. D., and Masters, M. M., "Investigating five key predictive text entry with combined distance and keystroke modelling," *Personal Ubiquitous Comput.,* vol. 12, no. 8, pp. 589-598, 2008.

[12] Dunlop, M. D., and Taylor, F., "Tactile feedback for predictive text entry," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2257-2260, 2009.

[13] Dunphy, P., and Olivier, P., "On automated image choice for secure and usable graphical passwords," *Proceedings of the 28th Annual Computer Security Applications Conference* pp. 99-108, 2012.

[14] Findlater, L., Lee, B., and Wobbrock, J., "Beyond QWERTY: augmenting touch screen keyboards with multi-touch gestures for non-alphanumeric input," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2679-2682, 2012.

[15] Gkoumas, A., Komninos, A., and Garofalakis, J., "Usability of Visibly Adaptive Smartphone keyboard layouts," *Proceedings of the 20th Pan-Hellenic Conference on Informatics*, pp. 1-6, 2016.

[16] Google. "Material Design Guildelines," May 5, 2018; https://material.io/design/layout/understanding-layout.html#usage.

[17] Hevner, A. R., March, S. T., Park, J., and Ram, S., "Design Science in Information Systems Research," *Management Information Systems Quarterly,* vol. 28, no. 1, 2004.

[18] Horcher, A.-M., and Tejay, G. P., "Building a better password: the role of cognitive load in information security training," *Proceedings of the 2009 IEEE international conference on Intelligence and security informatics* pp. 113-118, 2009.

[19] Huh, J. H., Kim, H., Rayala, S. S. V. P., Bobba, R. B., and Beznosov, K., "I'm too Busy to Reset my LinkedIn Password: On the Effectiveness of Password Reset Emails," *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pp. 387-391, 2017.

[20] Im, G. P., and Baskerville, R. L., "A longitudinal study of information system threat categories: the enduring problem of human error," *SIGMIS Database,* vol. 36, no. 4, pp. 68-79, 2005.

[21] ISO 9241, "Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs) Part 11:Guidance on Usability.," I. S. Organization, ed., 1998.

[22] Jain, A., and Chandra, M., "Heuristics-based algorithm to dynamically adapt icon sizes and layouts on touch devices," *SIGSOFT Softw. Eng. Notes,* vol. 39, no. 5, pp. 1-6, 2014.

[23] Jokela, T., Iivari, N., Matero, J., and Karukka, M., "The standard of user-centered design and the standard definition of usability: analyzing ISO 13407 against ISO 9241-11," *Proceedings of the Latin American conference on Human-computer interaction*, pp. 53-60, 2003.

[24] Kim, J. H., Aulck, L., Bartha, M. C., Harper, C. A., and Johnson, P. W., "Differences in typing forces, muscle activity, comfort, and typing performance among virtual, notebook, and desktop keyboards," *Appl Ergon,* vol. 45, no. 6, pp. 1406-13, Nov, 2014.

[25] Kim, J. H., Aulck, L., Thamsuwan, O., Bartha, M. C., and Johnson, P. W., "The effect of key size of touch screen virtual keyboards on productivity, usability, and typing biomechanics," *Hum Factors,* vol. 56, no. 7, pp. 1235-48, Nov, 2014.

[26] Kwon, S., Lee, D., and Chung, M. K., "Effect of key size and activation area on the performance of a regional error correction method in a touch-screen QWERTY keyboard," *International Journal of Industrial Ergonomics,* vol. 39, no. 5, pp. 888-893, 9//, 2009.

[27] Leftheriotis, I., "User authentication in a multi-touch surface: a chord password system," *CHI '13 Extended Abstracts on Human Factors in Computing Systems*, pp. 1725-1730, 2013.

[28] Lin, J., Sadeh, N., Amini, S., Lindqvist, J., Hong, J. I., and Zhang, J., "Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing," *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, pp. 501-510, 2012.

[29] Marasco, E., and Ross, A., "A Survey on Antispoofing Schemes for Fingerprint Recognition Systems," *ACM Comput. Surv.,* vol. 47, no. 2, pp. 1-36, 2014.

[30] Melicher, W., Kurilova, D., Segreti, S. M., Kalvani, P., Shay, R., Ur, B., Bauer, L., Christin, N., Cranor, L. F., and Mazurek, M. L., "Usability and Security of Text Passwords on Mobile Devices," *Proceedings of*

the 2016 CHI Conference on Human Factors in Computing Systems, pp. 527-539, 2016.

[31] Moore, P. "Passwords: Using 3 Random Words Is A Really Bad Idea!," June 1, 2018; https://paul.reviews/passwords-why-using-3-random-words-is-a-really-bad-idea/.

[32] Nielsen, J. "Guerrilla HCI: Using discount usability engineering to penetrate the intimidation barrier," December 11, 2009; http://www.useit.com/papers/guerrilla_hci.html.

[33] Oberheide, J., and Jahanian, F., "When mobile is harder than fixed (and vice versa): Demystifying security challenges in mobile environments," *Proceedings of the Eleventh Workshop on Mobile Computing Systems No. 38; Applications*, pp. 43-48, 2010.

[34] Oney, S., Harrison, C., Ogan, A., and Wiese, J., "ZoomBoard: a diminutive qwerty soft keyboard using iterative zooming for ultra-small devices," pp. 2799–2802, 2013, 2013.

[35] Parhi, P., Karlson, A. K., and Bederson, B. B., "Target size study for one-handed thumb use on small touchscreen devices," *Proceedings of the 8th conference on Human-computer interaction with mobile devices and services* pp. 203-210, 2006.

[36] Park, Y. S., and Han, S. H., "Touch key design for one-handed thumb interaction with a mobile phone: Effects of touch key size and touch key location," *International Journal of Industrial Ergonomics,* vol. In Press, Corrected Proof, 2009.

[37] Rick, J., "Performance optimizations of virtual keyboards for stroke-based text entry on a touch-based tabletop," *Proceedings of the 23nd annual ACM symposium on User interface software and technology*, pp. 77-86, 2010.

[38] Sandnes, F. E., "Reflective Text Entry: A Simple Low Effort Predictive Input Method Based on Flexible Abbreviations," *Procedia Computer Science,* vol. 67, pp. 105-112, 2015/01/01, 2015.

[39] Schaub, F., Deyhle, R., and Weber, M., "Password entry usability and shoulder surfing susceptibility on different smartphone platforms," *Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia*, pp. 1-10, 2012.

[40] Schaub, F., Walch, M., Konings, B. and Weber, M., "Exploring the design space of graphical passwords on smartphones," *Proceedings of the Ninth Symposium on Usable Privacy and Security*, pp. 1-14, 2013.

[41] Shirazi, A. S., Henze, N., Dingler, T., Kunze, K., and Schmidt, A., "Upright or sideways?: analysis of smartphone postures in the wild," *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*, pp. 362-371, 2013.

[42] Shneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., Elmqvist, N., and Diakopoulos, N., *Designing the user interface: strategies for effective human-computer interaction*: Pearson, 2016.

[43] Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J., "Analysis of end user security behaviors," *Computers & Security,* vol. 24, no. 2, pp. 124-133, 2005.

[44] Trinh, H., Waller, A., Vertanen, K., Kristensson, P. O., and Hanson, V. L., "Phoneme-based predictive text entry interface," *Proceedings of the 16th international ACM SIGACCESS conference on Computers & accessibility*, pp. 351-352, 2014.

[45] Vaishnavi, V., and Kuechler, B. "Design Science Research in Information Systems," October 3, 2011; http://desrist.org/desrist

[46] Varcholik, P. D., LaViola Jr, J. J., and Hughes, C. E., "Establishing a baseline for text entry for a multi-touch virtual keyboard," *International Journal of Human-Computer Studies,* vol. 70, no. 10, pp. 657-672, 2012.

[47] Yin, D. B. M., Omar, S., Talip, B. A., Muklas, A., Norain, N. A. M., and Othman, A. T., "Fusion of face recognition and facial expression detection for authentication: a proposed model," *Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication*, pp. 1-8, 2017.