Passwords and Interfaces: Towards Creating Stronger Passwords by Using Mobile Phone Handsets

S M Taiabul Haque[#] Matthew Wright[#] Shannon Scielzo[*]
eresh03@gmail.com, mwright@cse.uta.edu, scielzo@uta.edu
[#]Department of Computer Science and Engineering
[*]Department of Psychology
University of Texas at Arlington, USA

ABSTRACT

Entering a password on a mobile phone requires more effort than entering it on a PC keyboard, especially when using capital letters, digits, and special characters that are considered important for strong passwords. In this study, we examine how these factors affect the construction of passwords on input-constrained devices such as mobile phones. We conducted a between-group experiment with 72 students from the University of Texas at Arlington (UTA), in which we asked the participants to construct new passwords using PC keyboards and mobile phones with different keypad layouts. Passwords constructed by using PC keyboards were stronger than those constructed by touchscreen keypads. Surprisingly, passwords that were constructed by mobile phones with physical keyboards were stronger than those constructed by PC keyboards. We also designed a custom layout for the touchscreen keypad that offers a more convenient method of typing digits and some special characters. Our results show that this custom layout helped the participants to construct stronger passwords on mobile phones. To address an alternative explanation for better performance of the physical keyboard and custom layout groups, we designed a second experiment by removing the potential bias effects of the first experiment. The results of this within-group experiment confirm that if users are presented with a more convenient method of entering digits and special characters on mobile handsets, they take advantage of it to construct stronger passwords. The results also supplement our finding regarding password construction and user engagement from the first experiment and highlight an important design consideration about password construction pages for mobile versions of websites.

Categories and Subject Descriptors

D.4.6 [**Security and Protection**]: Authentication; H.1.2 [**User/Machine Systems**]: Human Factors

SPSM'13, November 8, 2013, Berlin, Germany.

http://dx.doi.org/10.1145/2516760.2516767.

General Terms

Security, Human Factors

Keywords

Passwords; handsets; interface; user study

1. INTRODUCTION

Password entry is a time-consuming and error-prone operation on mobile handsets. Jakobsson et al. report that password entry on handsets frustrates users more than lack of coverage, small screen size, or poor voice quality [6].

This poor user experience raises an important research question: "How do input-constrained devices like mobile phone handsets affect the password behavior of users?". In general, security experts say that a good password includes a combination of uppercase and lowercase letters, digits, and special characters[1]. Capitalizing a lowercase letter or inserting a digit on a mobile phone handset is not as straightforward as it is on a computer keyboard. On an iPhone, for example, each shift to and from digits requires one extra click and presents a different keyboard view to the user. Since the auto-correction and the auto-completion options of mobile handsets are not enabled for the password field, the general convenience of typing a password is also less on a handset than a computer.

These limitations suggest that passwords that are constructed by using mobile handsets would be relatively weaker than those constructed by using computer keyboards. However, there exists no empirical work in the current literature that examines the association between the strength of a password and the interface through which it is constructed. Moreover, keyboards on mobile handsets can also be classified into two categories, touchscreens and physical keyboards, which present users with two different password entry experiences. A handset with a touchscreen keypad is generally a high-end handset where a virtual keypad is available via the device's display screen. It uses touchscreen technology to enable a user to perform inputs by touching keys that appear on the screen. On the other hand, a handset with a physical keyboard has a built-in hardware keyboard, which is a smaller, modified version of a traditional computer keyboard.

The goal of our research is to examine how password strengths vary with the keyboard or keypad layout through which they are constructed. We are also interested to ob-

[1]See, e.g., `http://www.us-cert.gov/ncas/tips/st04-002`

serve the behavior of users when they are presented with a more convenient interface to construct passwords on a mobile handset. Therefore, we designed and evaluated the effectiveness of a custom layout that presented the users a more convenient option to insert digits and special characters while constructing a password.

We recruited 72 participants from the University of Texas at Arlington (UTA) and conducted a between-group laboratory experiment. Our purpose was twofold: to examine how password strengths vary across different interfaces and to test the effectiveness of our custom layout. We also conducted a second experiment that attempted to address a plausible alternative explanation regarding the results of the first experiment. This within-group laboratory experiment involved 24 UTA students as participants. The participants were rewarded for their time and the complete study was approved by the UTA Institutional Review Board (IRB).

2. RELATED WORK

Prior reseach has shown that text entry requires more effort on mobile phones. Bao et al. report that typing speed is significantly slower on phones than on PCs [1]. General observation suggests that capitalizing a letter and inserting digits/special characters also require more effort on a phone than on a computer. To date, however, no empirical work has examined how these factors actually affect the construction of passwords on computers and mobile phones. To the best of our knowledge, ours is the first empirical study that examines how password strengths vary across computer keyboards and mobile phones of different layouts.

Our proposed custom layout also provides a novel mechanism for inserting digits and special characters while constructing a password. Related works have mainly focused on improving the general typing speed on mobile phones. For example, proposals have been made for adding *chording* to numeric feature phone keypads [8, 12]. Other works have focused on pressure-based text entry [3, 10], but pressure-based schemes are often error-prone.

Chiang et al. [4] and Schaub et al. [9] evaluated the usability of graphical password schemes on smartphones, but graphical passwords have yet to replace textual passwords as a primary authentication mechanism.

Jakobsson and Akavipat propose to take advantage of the auto-correction and auto-completion features of mobile handsets with a mechanism called *fastword*, which is two to three times faster to enter than an ordinary password [5]. Their experimental results showed that fastwords have greater entropy and higher recall rates than ordinary passwords. Unfortunately, *fastword* is not fully compatible with existing sites that have arbitrary limits on password length and may require special characters, digits, and capital letters. Our proposed custom layout aims to assist users to enter digits and special characters in a more convenient way.

3. EXPERIMENT 1

In February 2013, we conducted a laboratory experiment with 72 UTA students (45 female and 27 male).

3.1 Study Administration

We administered the study through the *research pool* of the Department of Psychology at UTA. The pool is used to assign partial course credits to students taking "Introduction to Psychology" and extra credit for some advanced elective courses. The main advantage of putting a study in the pool is that it can draw a diverse set of participants, because most of these courses are offered to majors from all departments.

We also recruited participants (N=9) from outside the pool and offered them a restaurant gift voucher ($5).

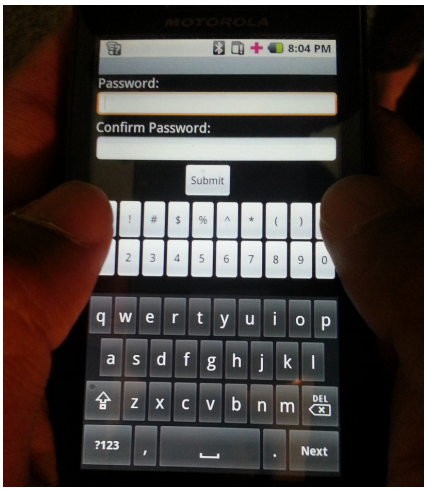

Figure 1: Custom layout with two extra rows of keys for digits and special characters.

3.2 Apparatus

For our experiment, we used a Motorola MILESTONE A853 mobile handset running Android 2.1. This handset contains a slide-out physical keyboard and also a QWERTY-type touchscreen keypad.

We designed our custom touchscreen layout by adding two extra rows of characters on the screen, as shown in Figure 1. One row contained the ten digits and the other row contained ten *common special characters*. These common special characters are the ten characters that appear along with the ten numeric keys on the second row of a standard desktop keyboard. The size and the inter-key distance of the additional keys were same as the original keys.

3.3 Experimental Groups

In our experiment, we asked the participants to construct new passwords. It was a between-group experiment and each participant constructed passwords by using one interface only. We randomly assigned each participant to one of the four groups:

- Computer keyboard (*keyboard* group)
- Mobile phone with physical keyboard (*physical* group)
- Mobile phone with touchscreen keypad (*touchscreen* group)
- Mobile phone with custom layout (*custom* group)

The *keyboard* group was provided with a standard PC keyboard. The other three groups were given the Motorola MILESTONE handset, but they were presented with different keyboard layouts. Since all three groups used the same device to construct passwords, confounding effects like the convenience of holding the device were removed.

As can be seen in Figure 1, digits and our selected special characters can be inserted with just one click in our custom layout, with no switching between layouts. On the other hand, inserting digits or special characters in the touchscreen

layout requires pressing the left bottom key first (the key labeled as "?123"), which would present the users a different layout view consisting of digits and special character keys only. For the physical keyboard layout, digits and special characters can be inserted by using the "ALT" key in conjunction with the regular letter keys.

3.4 Password Construction

The participants from each group were asked to construct new passwords using their respective interfaces for two different banking websites: Chase.com and Wellsfargo.com. We wanted the participants to spontaneously construct secure passwords that would be relatively long and would contain digits, capital letters, and special characters. Therefore, we selected banking websites to trigger the sense that security is important without explicitly asking them to construct strong and secure passwords. We selected banks that should be familiar to the participant students due to the prevalence of their ATMs on the UTA campus.

For ethical and security reasons, we explicitly told the participants not to provide any of their existing passwords. For both websites, we provided a brief introduction and presented a real-life scenario to the participants. For Chase.com, the participants were presented with the following scenario:

> Chase is one of the largest banks in the US and it has an ATM on campus. Imagine that you are creating an account at Chase.com for online banking. You have reached the final step of creating your new account, and you need to create a password. Proceed to the next page to input your new password.

When they clicked OK, the password construction page appeared. Once they constructed the password for Chase.com, a similar scenario was shown for Wellsfargo.com.

After constructing the passwords, the participants were asked a few questions about their mobile handsets. Demographic questions were asked at the end of the study.

3.5 Results

We calculated the mean entropy of the passwords for each of the four interfaces. The entropy was calculated by using the formula entropy $H = L \cdot log_2 N$, an approximation of plain Shannon entropy, where L is the length of the password and N is the size of the alphabet. The alphabet size is the sum of the sizes of different character types, specifically:

- Lowercase letters: 26
- Uppercase letters: 26
- Digits: 10
- Common special characters: 10
- Uncommon special characters: 22

As mentioned before, the common special characters are the ten characters that we included in a separate row in our custom layout. We distinguished between common and uncommon special characters so that an addition of a common special character from the custom layout would not unduly increase the entropy of the password (it increases the alphabet size by 10 instead of 32).

Figure 2 summarizes the entropy values for the four interfaces. As can be seen in Figure 2, The *touchscreen* group had lower entropy than the three other groups, and all four groups showed substantial variance.

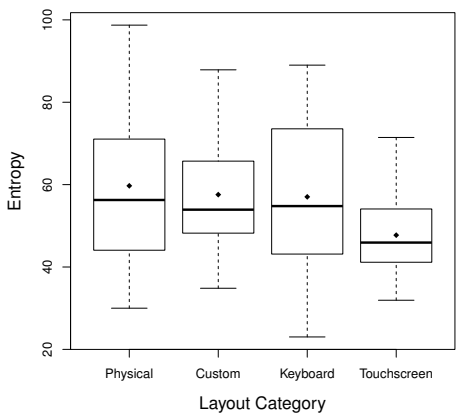

Figure 2: Box plot of entropy values. The mean entropy values are indicated by black dots.

Table 1: Summary of Tukey's post-hoc analysis. For each pair of interfaces, the difference, the 95% confidence interval and the p-value of the pairwise comparison are shown.

Pair	Diff	Lower	Upper	p-value
Custom-Keyboard	0.56	-9.37	10.48	0.999
Physical-Keyboard	2.90	-7.02	12.83	0.872
Touchscreen-Keyboard	-9.73	-19.65	0.20	0.057
Physical-Custom	2.35	-7.58	12.28	0.927
Touchscreen-Custom	-10.28	-20.21	-0.35	0.039
Touchscreen-Physical	-12.63	-22.56	-2.70	0.006

We conducted a one-way Anova test to analyze the differences between the mean entropies for the four interfaces. A one-way Anova test is the standard way to analyze the differences between more than two mean values. It is basically a generalization of the t-test for more than two groups, and helps to reduce the chance of incorrect findings of significance compared with multiple pairwise t-tests. The results demonstrated that entropy of passwords differed significantly across the four interfaces, $F(3, 140) = 4.28$, $p < .01$.

Since the difference value was significant for Anova, we also conducted Tukey's post-hoc comparisons to confirm where the differences occurred between groups. The results indicated that entropies were significantly higher for the *custom* group than those for the *touchscreen* group, $p < .05$. Also, the difference between the *physical* group and the *touchscreen* group was highly significant, $p < .01$. Table 1 summarizes the results for the Tukey's post-hoc test.

We conducted another one-way Anova test to compare between keyboard (*physical* and *keyboard* groups combined) and keypad (*touchscreen* and *custom* groups combined) interfaces. As predicted, entropies were significantly higher for the keyboard interface than those for the keypad interface, $F(1, 142) = 4.80$, $p < .05$.

3.6 Discussion

The design and the results of the first experiment left room for an alternative explanation for better performance of *custom* and *physical* groups. The experimental results demonstrated that the *physical* group created stronger passwords than the *keyboard* group. One possible reason for this might be the fact that, among the four interfaces, computer key-

boards are the most widespread. The participants of the *keyboard* group were already familiar with the interface and therefore were relatively less engaged in their password construction activity. As a result, the mean entropy was lower for *keyboard* group than *physical* group.

This same bias would apply to the *custom* vs. *touchscreen* comparison since people are more familiar with the standard touchscreen than the custom touchscreen. Thus, the alternative explanation for the better performance of our custom layout could be phrased as: "If mobile layout designers really were to adopt the custom layout, would users would become accustomed to it, causing it to lose its advantage?".

The reason for *physical* group's better performance than the *touchscreen* group could also be explained in this way. Our post-experimental brief survey regarding handset usage confirmed that a majority of the participants (47 out of 72) primarily use mobile handsets with touchscreen keypads. Thus, our sample population for Experiment 1 was predominantly familiar with touchscreen keypads, resulting in the same potential bias for *physical* vs. *touchscreen* group.

Experiment 2 was designed to address both of these alternative explanations by adding artificial tasks that required the participants to become accustomed to the interfaces before getting to the password creation task. Before creating passwords, participants were asked to complete other formalities of creating a new bank account. This, in turn, ensured that all the participants were already accustomed to the interfaces before creating the passwords, and allowed for a more fair comparison. A supplementary feature of Experiment 2 is that it was designed as a within-group experiment where each participant was asked to construct passwords by using two interfaces, which allowed for a more straightforward comparison between the interfaces.

4. EXPERIMENT 2

In June 2013, we conducted a second laboratory experiment with 24 students (14 female and 10 male). As with Experiment 1, we recruited participants from the research pool of UTA and used the Motorola MILESTONE A853 mobile handset.

4.1 Password Construction

In Experiment 2, we exclusively focused on comparing the standard touchscreen with the two other mobile phone layouts: physical keyboard layout and our custom touchscreen layout. This yielded two experimental groups and each participant was randomly assigned to one of the groups:

- Standard touchscreen vs. custom touchscreen
- Standard touchscreen vs. physical keyboard

4.1.1 Standard Touchscreen vs. Custom Touchscreen

The participants in this group were first presented with the following instructions:

> Chase is one of the largest banks in the US and it has an ATM on campus. Imagine that you are creating an account at Chase.com for online banking. Proceed to the next page to start creating your new bank account.

When a participant clicked OK, she was presented with a set of artificial tasks to be completed using the first layout she had been assigned. The tasks were designed so that they would resemble the usual steps of creating a new bank account. Users entered assigned dummy values, written on a piece of paper, for name, account number, address, and email address. The assigned address contained multiple special characters. Thus, while typing these dummy values, the participants got accustomed to typing capital letters, digits, and special characters in their respective interfaces.

After entering these dummy values, participants were asked to answer some questions like "How much daily withdrawal limit do you want?". Finally, they were redirected to the password construction page[2]. Once the password was constructed, the following message was displayed:

> Thank you for registering a new online account with Chase.com. For getting the full benefit of our online banking, we would like you to enroll in our ChaseQuickPay service. With Chase person-to-person QuickPay service, you can send money freely to anyone using their email address or mobile number.
>
> Proceed to the next page to start the enrolling procedure in ChaseQuickPay service.

When the participants clicked OK, additional artificial tasks were provided. This time, users were required to use the second assigned keyboard layout to satisfy the within-group condition. As with the Chase account, the participants were asked to enter the same dummy name, address, and email address, plus a different account number (called the ChaseQuickPay ID). They were also asked to answer a few questions like "How much daily transfer limit do you want?". After completing all these steps, they were redirected to the password construction page for the ChaseQuickPay service and specifically asked to construct a new password that would be different from the previous Chase bank account password.

We randomized the order of presenting the layouts to the participants. Thus, half of the participants constructed the Chase password by using the standard layout and the ChaseQuickPay password by using the custom layout. The remaining half followed the opposite order.

4.1.2 Standard Touchscreen vs. Physical Keyboard

Note that the participants of the previous group did not require switching the interface since both of the layouts were identical except the presence/absence of two additional rows of digits and special characters. However, participants were required to switch between the keypad and keyboard layout of the same handset in this group.

To provide a plausible cover story for switching the interface in the middle of the experiment, we intentionally disabled the OK button when the ChaseQuickPay service message was displayed. As a result, participants were unable to proceed to the next step. At this point, the experimenter manually intervened and took the device from the participant. The experimenter pretended that the system had frozen for that interface, apologized to the participant, and asked her to complete the ChaseQuickPay registration formalities in the second interface. The post-experimental debriefing session showed that only a single participant realized that this was an experimental manipulation for providing a plausible reason for switching the interface in the middle of the experiment.

[2]As before, the participants were asked not to provide any of their existing passwords.

All the other procedures followed by this group were identical to those followed by the previous group.

4.2 Results

We used a paired t-test to compare the entropy values in standard touchscreen and custom touchscreen conditions. The results showed that entropy values were significantly higher for custom touchscreen condition (M=53.88, SD=7.75) than standard touchscreen condition (M=45.77, SD=9.69); t(11)=2.45, p=0.03.

We also used a paired t-test to compare the entropy values in standard touchscreen and physical keyboard conditions. There was no significant difference in the scores for standard touchscreen (M=42.21, SD=7.38) and physical keyboard (M=45.67, SD=11.98) conditions; t(11)=1.02, p=0.33.

Finally, we carried out a paired t-test to compare the number of digits and special characters used by the participants in the standard touchscreen and custom touchscreen conditions. The numbers were significantly higher for the custom touchscreen condition (M=3.92, SD=1.38) than the standard touchscreen condition (M=2.33, SD=1.67); t(11)=2.78, p=0.02. This confirms that our custom layout primed the participants to use more digits and special characters in their passwords.

4.3 Discussion

As with Experiment 1, our custom layout resulted in the creation of passwords with significantly higher entropy values than the standard touchscreen layout. The custom layout was introduced so that participants could enter digits and special characters in a more convenient way. We predicted that passwords constructed by the custom layout would contain more digits and special characters than those constructed by the standard layout. This was in fact the result.

On the other hand, entropy values did not differ significantly between the standard touchscreen and physical keyboard conditions. This indicates that the advantage of physical keyboard over standard touchscreen in Experiment 1 might have been an artifact of the design methodology. In Experiment 1, some of the participants who used the physical keyboard layout (*physical* group) were likely more engaged during the password construction period since they were getting used to a less frequently used layout. In contrast, by the time the participants had reached the step of constructing a password by using a physical keyboard in Experiment 2, they were already familiar with the layout. As a result, they were relatively less engaged during the password construction period, which might have resulted in creation of passwords with lower entropies.

To further validate this, we performed a cross-experiment entropy comparison. The results showed that while the mean entropy did not vary much between the *touchscreen* group of Experiment 1 (M=48.26) and standard touchscreen conditions of Experiment 2 (M=44), it reduced drastically from the *physical* group of Experiment 1 (M=59.89) to the physical keyboard condition of Experiment 2 (M=45.67). An unpaired t-test showed a significant difference in the scores: $t(46) = 2.31$, $p = 0.025$. This suggests that user engagement is a significant factor in the password construction process.

Two issues are worth mentioning regarding the methodology of Experiment 2. First, participants of the second group were required to switch interfaces in the middle of the experiment, and this may have impacted their performances. However, we note that half of the participants switched from touchscreen keypad to physical keyboard, while the remaining half switched from physical keyboard to touchscreen keypad. Thus, the effects of switching affected both interfaces equally. Second, we did not conduct a *custom* vs. *physical* group comparison in Experiment 2. As the main objective of Experiment 2 was to explore the potential bias effect of Experiment 1, and since the results of the *touchscreen* vs. *physical* group comparison confirmed the existence of this bias, we deemed a *custom* vs. *physical* group comparison unnecessary. We also wanted to make a straightforward comparison between our custom layout and the standard layout.

4.4 Exit Survey

The final step for the participants was to fill a brief exit survey questionnaire regarding their password behaviors on mobile phones.

At first we asked the participants "On average, how much time do you spend every day in browsing the Internet through your mobile phone handset?". Out of 24 participants, 11 participants said that they spend "more than ten minutes but less than an hour", while 8 participants reported that they spend "more than an hour". Only 5 participants reported that they spend "less than ten minutes" on average each day. These responses clearly suggest that mobile browsing is a common task for most of our study's participants.

Next we asked the participants "When you create a new password for any online account on your computer, what factors do you take into account?". We provided multiple options such as "I consider how easy it is to remember", "I relate the password with the site", etc., along with the option of interest to our study: "I consider that at some point in the future, I might need to access that online account from my mobile phone also." The participants were asked to check all the options that apply; the other options provided some cover as to the experimenter's intent. Exactly half of the participants (12 out of 24) checked this option. These participants were further asked how this consideration affects their constructed passwords on computers. Their responses are shown in Table 2.

The participants were also asked how frequently they create new passwords for Webmail/social networking sites or banking/financial sites through their mobile phone. Overall, 21% (5) and 38% (9) of participants reported that they "never" or "seldom", respectively, create a new password for these important sites through their mobile phone. On the other hand, 21% (5) and 17% (4) reported that they "sometimes" and "often", respectively, create a new password for these sites through their mobile phone. Only 4% (1) of participants reported that they "always" create a new password for these sites through their mobile phones.

These findings suggest that users do not frequently create new passwords for their important accounts by using mobile phones. However, when they create a password on a computer, some of them consider the fact that at some point in the future they might need to type that same password on a mobile phone also and this affects their password behavior. These users likely choose a weaker password (passwords that are shorter, and passwords that contain fewer uppercase letter, digits or special characters) that would be considerably easier to type on mobile phones.

Table 2: Factors that affect password construction on computers (multiple responses allowed).

Behavior	Frequency
I create a shorter password because it is not easy to type a long password on a mobile phone.	2
I use fewer uppercase letters in my password because it is not easy to type an uppercase letter on a mobile phone.	5
I use fewer digits in my password because it is not easy to insert a digit on a mobile phone.	5
I use fewer special characters in my password because it is not easy to insert a special character on a mobile phone.	6

5. GENERAL DISCUSSION

In this section, we first discuss the ecological validity of our study. Next, we discuss limitations of our study and implications of our findings. We also shed light on future research directions.

5.1 Ecological Validity

It is difficult to demonstrate ecological validity [2] in any password study where participants are aware that they are creating passwords for an experiment, rather than for accounts that they value in real life for long-term use. Indeed, as we did not ask the participants in our study to return on a second day to re-enter their passwords, they were aware of the fact that there would be no consequences of their password choices. This might have impacted their password creation, since they had little incentive to create more memorable, and thus less secure, passwords.

We note that in our study, however, passwords for layouts of different categories were created under conditions that should be affected equally by this issue. Thus, we believe that the lack of a memorability test is not a critical issue for our study. Also, Komanduri et al. show that involving a role-play scenario as opposed to a survey scenario motivates users to construct passwords more seriously [7].

5.2 Low Sample Size

The sample size of our studies was not very large. For this reason, any attempt to generalize our findings to the broader community should be made with care.

5.3 Custom Layout

We have not conducted a full evaluation of our proposed custom layout. We designed the layout only to observe the behavior of the participants when they are presented with a more convenient option of inserting digits and special characters. Our results showed that the layout primed users to use more digits and special characters in their passwords, which in turn resulted in passwords with higher entropy values. Further research should be conducted before modifying the layout for mobile phones with touchscreen keypads.

In particular, our proposed custom layout has a limitation: it blocks the bottom part of the mobile phone screen. We note, however, that most existing password construction and password entry pages leave a considerable amount of blank space at the bottom of the page. Our custom layout, therefore, should not block any important portion of such pages during password entry. We plan to conduct a detailed usability study of our custom layout in the future.

5.4 Password Strength Measurement

We are aware of the fact that entropy is not the most appropriate measure of password strength [11]. For our studies, however, we mainly seek to capture how users' password behavior is constrained by keyboard layouts. The use (or lack thereof) of a variety of character types is captured reasonably well by our approximation of Shannon's entropy. Thus, we believe that entropy is more appropriate than measures such as difficulty of cracking, which is more dependent on the exact password choices of users than their ability to enter different types of passwords.

5.5 Mobile Interface and User Engagement

Our results from Experiment 1 showed, and those from Experiment 2 further supplemented, that users construct stronger passwords on interfaces that make them relatively more engaged in their password construction activity. This raises an interesting research question: "Should password construction interfaces be designed so that they make users more engaged in their password construction activity?". We plan to conduct research in this direction in future.

6. REFERENCES

[1] P. Bao, J. Pierce, S. Whittaker, and S. Zhai. Smart phone use by non-mobile business users. In *MobileHCI*, 2011.

[2] M. B. Brewer. Research design and issues of validity. In *H. T. Reis and C. M. Judd (Eds.), Handbook of research methods in social and personality psychology*, pages 3–16. New York: Cambridge University Press, 2000.

[3] S. A. Brewster and M. Hughes. Pressure-based text entry for mobile devices. In *MobileHCI*, 2009.

[4] H.-Y. Chiang and S. Chiasson. Improving user authentication on mobile devices: A touchscreen graphical password. In *MobileHCI*, 2013.

[5] M. Jakobsson and R. Akapivat. Rethinking passwords to adapt to constrained keyboards. In *MoST*, 2012.

[6] M. Jakobsson, E. Shi, P. Golle, and R. Chow. Implicit authentication for mobile devices. In *HotSec*, 2009.

[7] 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 *CHI*, 2011.

[8] N. Patel, J. Clawson, and T. Starner. A model of two-thumb chording on a phone keypad. In *MobileHCI*, 2009.

[9] F. Schaub, M. Walch, B. Konings, and M. Weber. Exploring the design space of graphical passwords on smartphones. In *SOUPS*, 2013.

[10] H. Tang, D. J. Beebe, and A. F. Cramer. A multilevel input system with force-sensitive elements. *International Journal of Human-Computer Studies*, 54(4):495–507, April 2001.

[11] M. Weir, S. Aggarwal, M. Collins, and H. Stern. Testing metrics for password creation policies by attacking large sets of revealed passwords. In *CCS*, 2010.

[12] D. Wigdor and R. Balakrishnan. A comparison of consecutive and concurrent input text entry techniques for mobile phones. In *CHI*, 2004.