Efficiency and Device Versatility of Graphical and Textual Passwords

Completed Research Paper

Dugald Ralph Hutchings
Elon University
dhutchings@elon.edu

David Steven Williams Jr.
Elon University
dwilliams22@elon.edu

ABSTRACT

We present the design, execution, and results of a user study of entry speed and error rate of a variety of password schemes used on a variety of computing platforms. A standard text-based password, a personal identification number (PIN), and three different graphical password systems were designed and deployed for use and evaluation on each of a desktop computer, a touchscreen tablet, and a touchscreen phone. We demonstrate cases on the mobile devices in which the graphical approaches exhibited faster rates of entry than the complementary textual password approach. We make a case for the study of the *device versatility* of authentication mechanisms and discuss potential improvements to graphical approaches to achieve greater levels of efficiency.

Keywords

Graphical Passwords, Efficiency, Errors, Device Versatility

INTRODUCTION

The most common method for authenticating users to computing resources is the *password* technique, in which the resource in question stores a sequence of previously selected or assigned textual characters (often in encrypted format) that a user must exactly enter to gain access. The *password problem* refers to a fundamental tension between memorability and security that exists within this ubiquitous knowledge-based authentication mechanism. Passwords consisting of a few characters or pertaining to something about the user are easily remembered but also easily compromised by a malicious person. Long passwords that have no relationship to the user are much more difficult to compromise yet difficult for the user to remember, possibly leading to an inability to gain legitimate access to a resource. A good password must reside in an apparently narrow space of "easy to remember but hard to guess."

Researchers in the usability and security fields have endeavored to explore alternative mechanisms to the text-based password in an effort to heighten memorability, security, or both. Prominent among these efforts are techniques called *graphical password* systems that typically involve a user creating or interacting with some number of pictures in a sequential way in order to authenticate. For example, Komanduri and Hutchings developed a system in which a user selects from a number of on-screen images (Komanduri and Hutchings, 2008), quite similar to a user selecting from a number of textual characters on a keyboard. Systems such as Komanduri's and Hutchings's graphical approach exploit human memory properties to facilitate a more memorable authentication sequence relative to textual passwords.

Biddle's et al. recent work provides an extensive overview of the past decade of explorations of graphical password systems and related elements (Biddle, Chiasson, and van Oorschot, 2012). Three key observations of that overview drive the work performed in this paper:

1. although graphical passwords generally show superior memorability relative to textual passwords, graphical passwords generally show inferior *efficiency*, i.e., time required by the user to authenticate;
2. effects of *error rate*, i.e., likelihood of a user committing an error during authentication and needing to try again, are inconsistently measured and reported; and
3. *versatility*, i.e., the usability characteristics of graphical passwords across various computing platforms (and particularly mobile touchscreen devices) is unexamined.

With nearly half of all American adults owning a smartphone (Smith, 2012), and given the nearly identical *information access* capabilities of smaller mobile devices, it is worth examining how well both textual and graphical knowledge-based authentication mechanisms can be used via touchscreen. We have conducted a comparative study of efficiency, error rate, and

device versatility of a set of textual and graphical password techniques. Our study indicates that graphical techniques can be more efficient than a textual technique on mobile touchscreen devices as well as more efficient in aggregate (*i.e.*, when averaging results among all device types). We propose extending security-usability frameworks to consider cross-platform versatility as a key usability component of knowledge-based authentication mechanisms.

RELATED WORK

Biddle's et al. comprehensive survey of graphical passwords serves as the foundation of discussion in this section (Biddle et al., 2012). Readers unfamiliar with graphical passwords may find it fruitful to visit that work in its entirety. We provide discussion of only the directly relevant aspects of Biddle's et al. work: categorization of graphical password schemes; canonical and other examples in each category; and key past usability studies. The three main categories of graphical approaches are *recall*, *cued-recall*, and *recognition*.

Figure 1: On the left is a guide for a DAS prototype indicating lines to be drawn and the drawing sequence and direction. In the middle and right are two samples that, if drawn in the correct sequence and direction, would successfully authenticate the user.

Recall

Draw-A-Secret (DAS) is most similar to a typical textual password in that a user must provide a sketch using a grid that matches the number, sequence, and shape of lines in a previously sketched drawing (Jermyn, Mayer, Monrose, Reiter, and Rubin, 1999). In other words, the user must exactly *recall* the graphical password without any guidance. The user must start the sketch in the appropriate grid box, pass through a sequence of grid boxes, and end the sketch in the appropriate grid box for each line in the sketch (each grid box entered and each new line can be considered to be a character equivalent to textual password entry). Figure 1 demonstrates the interface. Both our review and Biddle's et al. review revealed no studies measuring efficiency, error rate, or device versatility of DAS nor its commercial variations such as Android's pattern lock, itself a less secure[1] approach than DAS (an equivalent comparison of DAS to Android pattern lock would be standard textual passwords to PINs).

[1] Throughout this paper we generally use *security* to refer to the number of unique combinations of sequences afforded by the password technique (i.e., the *password space*). *Entropy analysis*, typically used in security literature, is outside the relevant scope of our work and thus we avoid its discussion.

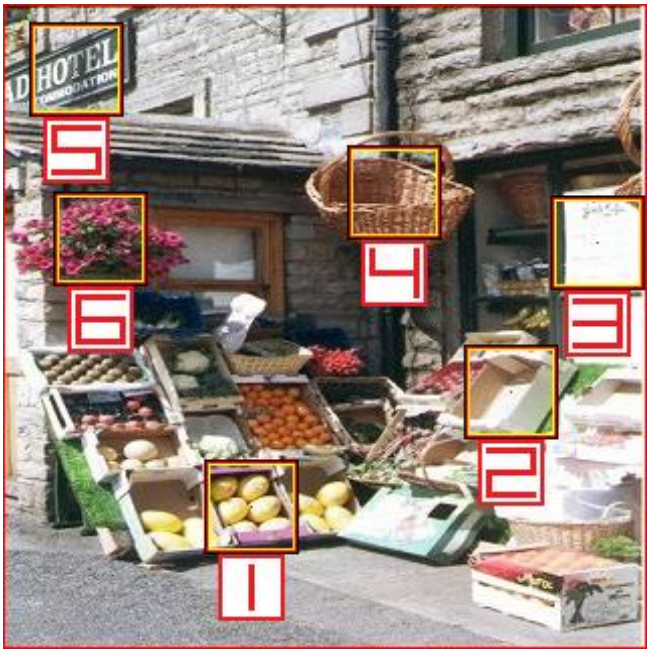

Figure 2: A sample PassPoints image with points, point tolerances, and point sequences marked by numbers and boxes.

Cued-Recall

PassPoints (Wiedenbeck, Waters, Birget, Brodskiy, and Memon, 2005a) is similar to DAS with two important differences: (1) instead of a blank grid, the user interacts on an image (typically a photograph); and (2) the user clicks or taps on distinct points in the image rather than making a sketch. The image and its visual components cue the user to tap on or near those components but otherwise give no hint as to the correct sequence of taps in the graphical password. PassPoints is also similar to DAS in that the user does not have to be pixel perfect; instead, the user must click or tap within a specified distance of the target pixel point for each point in the sequence. Figure 2 shows a sample image, point sequence, and tolerance size for PassPoints; during authentication the boxes and numbers do not appear.

At least three publications address unique PassPoints studies of login time. In Wiedenbeck's et al. report, a measure of quantity of erroneous attempts and the "time for correct submission" were consolidated using means, but it is unclear from the description of the results whether the recorded time included or excluded the time taken during the erroneous attempts (Wiedenbeck, Waters, Birget, Brodskiy, and Memon, 2005b). In a separate study, Wiedenbeck et al. assessed variations on the original PassPoints design and measured the quantity of erroneous attempts and time for correct submissions, but also included time for incorrect submissions (Wiedenbeck, et al., 2005a). Chiasson et al. studied the PassPoints approach through separate lab and field studies but used medians instead of mean times in the analysis (Chiasson, Biddle, and van Oorschot, 2007). Chiasson et al. also discuss *how* to measure time, noting that it is worth investigating the "click time," i.e., the time taken from first click to last click and separating it from other time that might be necessary (such as entering a user name or preparing to interact), an approach we follow in our study.

Figure 3: Four consecutive grids of faces (top area) and the password guide (bottom area, repeated) used in PassFaces. Each grid contains one face from the guide that the user must tap to log in.

Recognition

In the PassFaces approach, a user must select one face each from 4 consecutive grids of 9 pictures of different people's faces, making PassFaces more similar to PINs than passwords in terms of security and interaction (Passfaces, 2012). A difference however is that the ordering of face grids and the positions of faces within the grid vary upon each login attempt. In PassFaces, the user must *recognize* the one correct selection from a grid of 9 choices and do so 4 consecutive times. This distinction may seem arbitrary as compared to PINs, but note that the faces change in each consecutive grid and the degree of memorable features of a human face far outweighs memorable features of a single numeral. Figure 3 demonstrates the interaction sequence of a sample PassFaces application. Similar to DAS, our review and Biddle's et al. review of the literature reveals studies only of memorability, with no studies measuring efficiency nor device versatility.

Summary

Measurements of entry speed for proposed knowledge-based authentication mechanisms, especially graphical passwords, are often lacking but when they are available, show little consistency from study to study. Of the canonical examples in the three main categories of graphical passwords, only one has been directly compared to a textual password with a similar level of security and it was shown to be far slower than its textual counterpart. To our knowledge, no graphical password approach of any kind has been specifically examined for device versatility, i.e., usage across a variety of devices. Considering especially secured Web-based applications that may be accessed on a variety of devices, we strive to understand how quickly (efficiently, and with minimal errors) all of these viable password techniques can be used on different likely devices (versatility) and thus contribute to an important but lacking area of research on the usability of knowledge-based authentication mechanisms.

STUDY DESIGN

We endeavored to design a consistent comparison of the canonical examples of each of the three categories of graphical password systems to the two standard textual password approaches. From here forward, we capitalize and italicize the names of these techniques (*DAS, PassFaces, PassPoints, Password, PIN*) when we desire to refer to the specific technique. In particular we use *Password* to specifically refer to a sequence of alphanumeric or special characters, but use password (unitalicized, uncapitalized) to generally refer to any or all of the knowledge-based techniques. Below we give a brief overview of participant activities in the study, a rationale for some of the design decisions, and some noteworthy study details.

Study Overview

After providing some basic demographic information, participants in our study learned about and practiced each of the three graphical passwords using paper prototypes that were similar to the actual interfaces to be used later. The participant was then directed to one of three devices: (1) a desktop computer with keyboard and mouse; (2) a first-generation Apple iPad touchscreen tablet; or (3) a first-generation Apple iPod Touch (which is essentially an Apple iPhone touchscreen phone without the telecommunications component). The experimental software selected one of the password interfaces at random and displayed it on screen. A *password guide* displayed to the participant the password to be entered. After the participant entered the password two times successfully, the guide automatically disappeared. The participant then entered the password three times correctly (or made 10 total attempts, whichever came first). If the participant felt that he or she did not know or remember the password, the participant could click a *hint* button to undertake one additional training trial. This first password was considered to be practice in our study. The software then presented a second password and finally a third password in a random order, each involving two successful hint-aided practice entries and then timed entries until three successful logins or 10 total attempts occurred.

The set of five randomly presented password interfaces was likewise repeated for the remaining two hardware platforms. The presentation of hardware platforms was counterbalanced among the participants to mitigate learning effects. Since three hardware platforms are presented to users, there are six possible orderings of hardware presentation and the study design thus calls for a sample size divisible by 6 (ultimately we recruited 18 participants; see *Study Results* for additional information). For each group of six participants, the assignment of participant to a specific ordering of hardware platform was randomized. Summarizing, in this within-subjects design, we executed

3	successful logins for each of
2	passwords in each of
5	interfaces (*DAS*, *PassFaces*, *PassPoints*, *Password*, *PIN*) on
× 3	computing platforms (*desktop*, *phone*, *tablet*), totaling
90	timed trials (plus 45 additional untimed practice trials).
× 18	participants, for a grand total of
1620	timed trials

Design Rationale

Our overall goal in this study was a fair and consistent comparison of password techniques across different types of computing devices and our design choices reflect this overall goal. Three passwords, with the first one always being untimed practice, struck a balance between familiarity (with the device and interface pair) and the number of interfaces that could be studied in a one-hour session. Participant-assigned rather than participant-selected passwords struck a balance between consistent comparison (everyone entered the same passwords) and ecological validity (most password systems allow the user a fair degree of choice in selecting the password). Usage of a hint likewise struck a balance between ecological validity and the desired study metrics of efficiency. Other studies have addressed password choice (the *Background DAS* study (Dunphy and Yan, 2007), e.g.); we desired to analyze behavior when the password was known and practiced to some degree, so if a particular participant needed more training time, then the participant could elect to get it.

Password Selection

We attempted to craft passwords for each interface that met real-world criteria for creation (for example, textual passwords with three of the four following classes: lower-case letter, upper-case letter, number, and non-alphanumeric) but were also immediately memorable (for example, “tru5T1ng” looks like the word “trusting”). We do not necessarily propose that these are strong passwords, but rather that they are reasonable. Figure 4 shows all passwords used in the study.

Use of different passwords in any replicated or follow-up studies will quite likely provide different timing results and we encourage such work to help refine our findings. Ultimately, some passwords have to be selected for each technique and we selected passwords we believed to be fair to the technique and quickly memorable. An important point is that the same set of passwords was used on all three devices. The benefit of this approach is that cross-device comparison is much more direct but the drawback is a potential learning effect (participants are faster on devices used later in the study simply by virtue of practice on other devices). As previously noted, we aimed to mitigate this decision by fully counterbalancing the order in which participants used the devices.

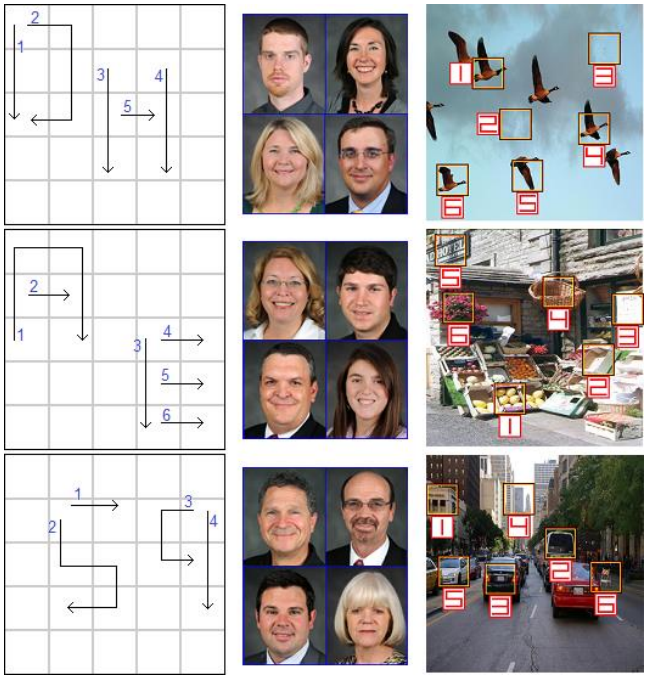

Figure 4: From left to right, the passwords used in *DAS*, *PassFaces*, *PassPoints*, *Password*, *and PIN* respectively. The images and text on the top row were used in the practice (non-timed) trials.

Interface Design

Each of the 5 interfaces was created to fit in the usable space of the phone when used in the portrait orientation (320px × 460px). Apple-specific HTML tags and attributes were used to fix the zoom level at 1:1 and to prevent the user from zooming the interface or changing the orientation of the device. The phone was presented to the user in the portrait orientation and the tablet was presented in landscape.

The top 16 pixels of each interface were used to show the participant the interaction history and progress through each password entry. A green box resembling a smiling face was inserted after a successful entry and a red box resembling a frowning face was inserted after an erroneous entry. Other icons were used to illustrate when practice ended and when hints were shown.

Design was carefully considered for the graphical interfaces. For example, the *DAS* password guide was shown below the sketch entry area whereas the *PassPoints* guide was shown overlaid on the tap/point entry area. The nature of the interfaces guided this decision: tapping a visually marked point should be easy but sketching over a visually indicated line could be more difficult, especially with one or more fingers occluding the parts of the line to be drawn next. This resulted in an entry area that was smaller for *DAS* (180px × 180px) than for *PassPoints* (318px × 318px). Future work should address the optimal ways to support password creation/learning so as to maximize the amount of available screen space as well as ways to safely scale the graphical techniques to a variety of screen sizes.

In *PassFaces*, the entry area was 270px × 330px, yielding face photograph sizes of 90px × 110px each. The password guide was a static image of 4 faces using 270px × 81px and each guide face was scaled down by 25% relative to the face used in the grid.

In all graphical password interfaces, a *start over* button allowed the participant to self-diagnose an entry error. Use of this button did not count against the maximum number of ten total entry attempts. In the textual interfaces, the participants could use the backspace key to erase some or all of the characters entered.

In the *PIN* interface condition, desktop users could use the top row of number keys or a keypad. On the phone, the dialing pad was used. On the tablet, participants had to use the built-in virtual keyboard screen with numbers at the top row.

STUDY RESULTS

Eighteen undergraduate students (11 female, average age 20.1 yrs) from our institution enrolled in the study. Four participants (22%) were enrolled in IT-related programs. All were owners of at least one mobile touchscreen device and all but one indicated that they used such devices multiple times every day (the other indicated using such a device once a day). Sixteen participants (89%) indicated that they frequently entered passwords or PINs on the mobile devices, with 11 of the 16 people indicating entry "nearly every time" they used the device. The participants are considered to be expert users of computing technology in general and mobile touchscreen technology specifically. Participants were not specifically polled as to their experiences with graphical passwords however in post-task interviews however, all participants affirmed that they had not used the specific techniques tested in the experiment prior to participation.

Time Calculation

Upon any entry (successful or not), a green or red box covered the password entry area for 1.5s and then the participant could proceed to make another entry. When using the *start over* button, a blue box covered the space for 1.5s and in the collected data, this was considered an unsuccessful entry, though it did not count against the 10 total attempts. There are four important time points in password entry: presentation of interface, first interaction (key down, mouse down, or touch start), last interaction (key up, mouse up, or touch end), and if applicable, confirmation (i.e., clicking the "login" button). Our view is that measurement for efficiency analysis should occur from first interaction to last interaction (similar to the "click time" analysis of Chiasson et al. (2007)). This eliminates any variability in preparation for entry, mouse location from the previous entry or at the end of interaction (if applicable), review of the interaction sequence, etc.

Another aspect of time calculation is how to account for unsuccessful logins. Suppose that an interface allows for rapid entry of the password, but participants frequently commit errors during entry. It seems inaccurate to report that this interface is efficient, because realistic login times will also include the time needed for the erroneous attempts. On the other hand, perhaps the errors are related to our specific implementation of the interface rather than inherent difficulty in executing the technique. Further, in our study when passwords and interfaces are changing frequently, an error may be the result of a genuine mistake (hitting the wrong key, tapping the wrong face) or the result of not actually knowing the password (believing that a PIN is 1829 instead of 1928 or tapping a distractor face with some similarity to the target face). Our approach of allowing the participants to show password hints provides a clue that participants are not confident in their knowledge of the passwords to be entered. Consequently, we omit all sequences of unsuccessful logins that precede the usage of the hint button and we shortly present two analyses: one that accounts only for the time needed in the successful attempts and another that accounts for both the unsuccessful and successful attempts.

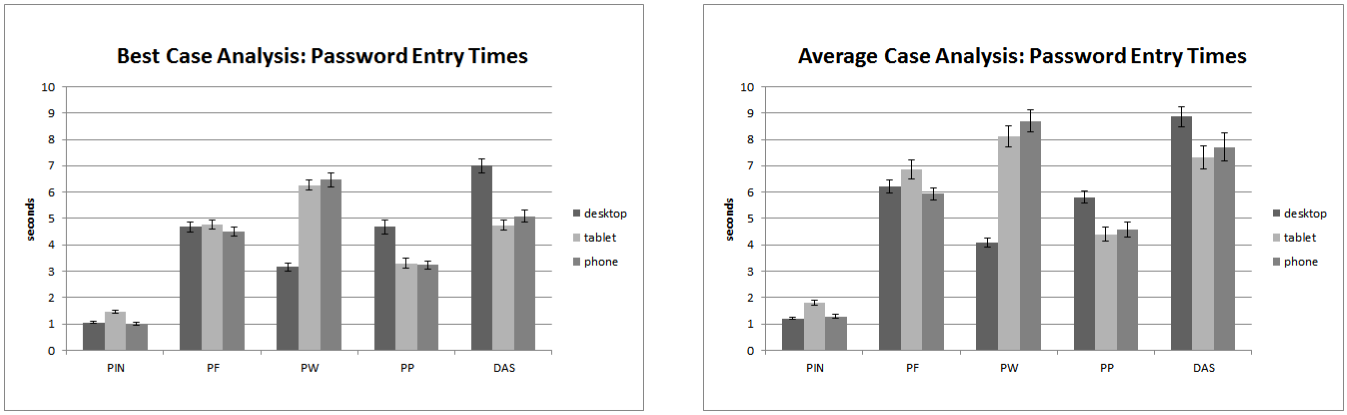

Figure 5: Login times in the best case (left) and average case (right) analyses. I-Bars indicate one standard error from the mean.

Efficiency Analysis

For each participant (18), device type (3), interface type (5), and password (2), a total of 540 distinct cases, we selected the successful login trial completed in shortest amount of time for *best-case analysis*. Data selection for *average case analysis* is similarly broken down by participant, device type, interface type, and password, but all trials are considered and as explained in the previous section, successive erroneous attempts preceding a successful attempt are combined to form a single trial. This results in 1617 trials for average case analysis (in 3 cases, participants were only able to login 2 times successfully).

Figure 5 illustrates the trial times from both analyses. There is great similarity in the two charts with the obvious difference being shorter login times in the best case analysis. Further, the reader should plainly see the speed dominance of *PIN* over all other techniques (particularly *PassFaces*, the only other technique with a similar level of security). Given the high level of similarity between the two analyses and the dominance of *PIN*, we undertook a more thorough statistical analysis of only the average case data for *Password* and the two security-equivalent techniques *DAS* and *PassPoints*.

A two-factor ANOVA with replication showed a significant main effect of device type ($F_{2,107}$=3.088, p=0.046), a significant main effect of interface ($F_{2,107}$=51.28, p<0.001) as well as an interaction effect ($F_{5,485}$=26.07, p<0.001). Expecting differences among the devices, we used post-hoc *t*-tests only for the interface-device combinations and aggregate interface data, using the conservative Bonferroni α correction. As suggested by Figure 5, significant differences were found for each interface when comparing desktop to either one of the touchscreen devices (except for *DAS* on desktop vs. phone), but no significant differences were found between the two touchscreen devices. With respect to aggregate interface analysis, *PassPoints* was significantly more efficient than *Password*, which in turn was significantly more efficient than *DAS*.

Our data analysis suggests that *Password* is relatively efficient when a full keyboard is available, but relatively inefficient on the mobile touchscreen devices. *PassPoints* and *DAS* are relatively more consistent but slower on the desktop. *PassPoints* is the most versatile: login times do not vary by much more than 1s across devices and is *overall* the fastest interface (5.0s overall vs. 7.0s overall for *Password*). This is the first known study to demonstrate an efficiency advantage for a graphical password technique.

	PIN	**PF**	**PW**	**PP**	**DAS**
Desktop	0.0	0.3	0.2	0.8	1.5
Tablet	0.1	0.6	0.4	1.4	2.7
Phone	0.2	0.2	0.6	1.6	2.9
Overall	0.1	0.4	0.4	1.3	2.4

Table 1: Mean Erroneous Attempts per Successful Login

	PIN	**PF**	**PW**	**PP**	**DAS**
Desktop	0	0	0	0.2	0.2
Tablet	0	0	0	0.2	0.3
Phone	0	0	0	0.2	0.3
Overall	0	0	0	0.2	0.3

Table 2: Median Erroneous Attempts per Successful Login

Error Analysis

A small number of participants accounted for a large number of errors exhibited in our study. The mean and median numbers of unsuccessful attempts preceding a successful attempt are displayed in Table 1 and Table 2, respectively. Looking particularly at *DAS* and *PassPoints*, we see high means but fairly low medians. Almost exactly half of all of the errors committed in these two interfaces came from 3 participants (just 17% of the overall sample). We infer from this analysis that for some participants, use of a graphical password technique requires additional training or practice, or is altogether inherently difficult to use relative to textual methods.

Regardless of the way participants committed errors, large error rates are problematic for password interfaces for a variety of reasons. A number of security systems employ a lockout mechanism in which account access is automatically disabled after a fixed number of successive erroneous attempts, forcing the user to have the password manually reset or in some cases with mobile devices, erasing the content on the device. Without revising the interfaces used in the study, the likelihood of lockout increases unless the number of attempts increases. Such an increase however could compromise the level of security (allow-

ing an attacker with partial knowledge of the password more attempts to login as the user). Further, any interface with a high number of errors can cause unneeded frustration.

Except for *PassFaces*, the number of errors committed by participants rose as the size of the input device decreased. This suggests consideration of a slight relaxation of the number of attempts prior to lockout on systems likely to be accessed by mobile devices.

Summary

PIN is a very fast mechanism unlikely to be supplanted by any graphical technique when the desired level of security is low. *Password* was the most efficient technique on the desktop but *PassPoints* was most efficient on mobile touchscreens, as well as in the aggregate analysis. *DAS* was slowest of all techniques in the aggregate, but not significantly slower than *Password* on the touchscreen. Participants exhibited that both *DAS* and *PassPoints* could be improved, likely leading to more efficient use of the interfaces.

DISCUSSION

A limitation of our findings and conclusions is that training or learning time for a password is not taken into account, nor is the time needed to devise a password for systems that allow user choice. The long-run efficiency of a technique likely depends on the policies instituted by organizations or systems surrounding password change. A technique that takes somewhat longer to learn but is very fast in practice may not be as efficient if the password must be changed every few weeks or months or is used only infrequently by the user. The time needed to actually change the password (especially when forgotten by the user) is also a factor. A more comprehensive investigation would take training, learning, and reset process times into account. Our findings are most directly relevant to passwords that are frequently used.

Another limitation of our study is that only two types of touchscreens and virtual keyboards were examined, each by the same manufacturer. Especially with text entry, variations in the on-screen keyboards can lead to very different entry times. As more and more users interact with a variety of computing devices on an everyday basis, users may tend toward crafting a *Password* that uses only characters from the first set of virtual keys, significantly limiting the actual level of security of the technique.

Despite the limitations of the presented study, we have shown that there is a case to be made for the use of graphical passwords, especially considering the rise in popularity and everyday use of touchscreen devices for secure computing applications. Biddle's et al. overview of graphical password work showed that graphical passwords have generally been observed to be relatively slow (Biddle et al., 2012) but we have shown a common case in which graphical passwords are relatively fast. By continuing to refine the techniques, even more efficient use is expected.

We also suggest with this work that knowledge-based authentication mechanisms be evaluated not only in terms of security, memorability, and efficiency, but also in terms of device versatility. Conversely, work could also proceed to provide interfaces that are designed from the ground up to operate equally efficiently in common computing environments and persuade users to create strong, memorable, and efficiently-entered passwords.

ACKNOWLEDGEMENT

We wish to thank Heather Richter Lipford for helpful commentary on early versions of this work.

REFERENCES

1. Biddle, R., Chiasson, S., and van Oorschot, P. C. (2012) Graphical passwords: learning from the first twelve years, *ACM Computing Surveys* 44, 4, Article 19, 41 pages.
2. Chiasson, S., Biddle, R., and van Oorschot, P. C. (2007) A second look at the usability of click-based graphical passwords in Lorrie Faith Cranor (Ed.) *Proceedings of the 3rd symposium on Usable privacy and security (SOUPS '07)*, July 18-20, Pittsburgh, PA, USA, ACM Press, 1-12.
3. Dunphy, P. and Yan, J. (2007) Do background images improve "draw a secret" graphical passwords? in Sabrina De Capitani di Vimercati, Paul Syverson, and David Evans (Eds.) *Proceedings of the 14th ACM conference on Computer and communications security (CCS '07)*, October 29 – November 2, Alexandria, VA, USA, ACM Press, 36-47.
4. Jermyn, I., Mayer, A., Monrose, F., Reiter, M., and Rubin, A. (1999) The design and analysis of graphical passwords in Win Treese (Ed.) *Proceedings of the 8th conference on USENIX Security Symposium (SSYM'99)*, August 23-26, Washington, DC, USA, USENIX Association, 1-14.
5. Komanduri, S. and Hutchings, D. R. (2008) Order and entropy in picture passwords, in Lyn Bartram and Chris Shaw (Eds.) *Proceedings of graphics interface 2008 (GI '08)*, May 28-30, Windsor, ON, Canada, Canadian Information Processing Society, 115-122.
6. Passfaces Corporation (accessed June 7, 2012) The science behind Passfaces (white paper). URL: http://www.passfaces.com/enterprise/resources/white_papers.htm
7. Smith, A. (accessed Mar 1, 2012) 46% of American adults are smartphone owners from the *Pew Internet & American Life Project*. URL: http://pewinternet.org/Reports/2012/ Smartphone-Update-2012.aspx
8. Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., and Memon, N. (2005) Authentication using graphical passwords: effects of tolerance and image choice in Lorrie Faith Cranor (Ed.) *Proceedings of the 2005 symposium on Usable privacy and security (SOUPS '05)*, July 6-8, Pittsburgh, PA, USA, 1-12.
9. Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., and Memon, N. (2005) PassPoints: design and longitudinal evaluation of a graphical password system, *International Journal of Human-Computer Studies*, 63, 1-2 (July 2005), 102-127.