Click to Enter: Comparing Graphical and Textual Passwords for Children

Jasper Cole
Digital Whimsy Lab
University of Baltimore
jaspercole@ubalt.edu

Greg Walsh
Digital Whimsy Lab
University of Baltimore
gwalsh@ubalt.edu

Zachary Pease
Digital Whimsy Lab
University of Baltimore
zacharypease@ubalt.edu

IDC '17, June 27-30, 2017, Stanford, CA, USA

ACM ISBN 978-1-4503-4921-5/17/06.
http://dx.doi.org/10.1145/3078072.3084311

Abstract
This work outlines a study comparing graphical and textual passwords. A study was conducted with 13 children between the ages of six and twelve years old. These participants created their own textual and graphical passwords for fictional Web sites and after two weeks, participants returned and attempted to recall the usernames and passwords that they created. Our preliminary results showed that graphical passwords had a lower success rate and participants were less likely to access their accounts when using graphical passwords. Whether using graphical or textual passwords, children succeeded with generalities, but struggled with specifics.

Author Keywords
Security; Passwords; Children

ACM Classification Keywords
D.4.6 [Security and Protection]: Authentication

Introduction
In their article Designing Textual Password Systems for Children, Read & Cassidy wrote “studies on how children create and use passwords are rare” [8]. These authors suggest requiring text passwords that do not require 8 letters and do not require a mixture of numbers, letters, and symbols, but they do not discuss any alternatives methods.

Figure 1: A participant is smiling while entering a graphical password on a picture of a motor bike.

Despite this, they write that “textual passwords can be especially problematic for children” (p. 200). Therefore, it is worthwhile to examine some other systems of authentication and their accessibility, memorability, and favorability among children. Alternative passwords may be better for children, providing safer, easier, and more secure access to their private information.

Graphical passwords are a popular alternative among adults and have been the subject of many studies. One of the most discussed system is PassPoints - where users select several distinct points on an image and then recall these positions accurately in order to access their account. This system has been studied extensively and many authors have written about it. For example, Wiedenbeck et al. [11] examine tolerance and image choice and Dirik & Birget [4] model and predict user choice. These studies are built around the potential viability of graphical passwords among adults.

Some research has been done on children and passwords already. Despite a long history of research about children’s struggles with passwords, and many viable alternatives, there are very few studies that compare alternative password systems to more conventional textual systems. This paper discusses one preliminary study into the use of one type of graphical password system with children.

Background

Research about children and computers has been mostly separated from research relating to passwords and login systems. These subjects have some overlap, but in general research about children is focused on design and usability [12]. Some research examines the effects of computer use on children’s development [1]. If children are going to use computers, they need to be able to use them securely. This means secure access through children-friendly login and password systems. Very little research looks seriously at the question of security and what security is appropriate and effective for children.

From the research that has been done, it is clear that researchers do not feel that children can use textual passwords effectively. Read & Cassidy [8] explain that children do not know how to create secure textual passwords and designers need to make many accommodations for children to use textual passwords. These accommodations may well compromise the security of the system. They end their article discussing that “future work will be looking at [...] the use of non-textual passwords for children”. Unfortunately they do not study or suggest any alternative password methods, and no one has yet identified any leading alternative methods for children’s passwords.

There has been some research published on alternative login methods for children. Mendori et al [7] posits a symbol based password as a child-friendly alternative to conventional textual passwords. Icon identification seems plausibly superior to textual passwords, but no comparisons were performed for memorability. Therefore, it is unclear if this type of password system performs better, the same, or worse than a conventional textual password.

Stemming from literature about adult users, there is an underlying assumption that textual passwords are inherently problematic and a superior login system could be created. Articles such as [6] outlines the ways password reuse compromises the security of textual password systems. In [10], the authors explain the harsh demands of textual password systems by showing how many user names and passwords adults are expected to remember, and exploring how frequently these passwords are forgotten. They recommend

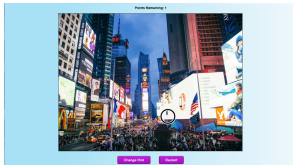

Figure 2: The graphical password screen in the second prototype. There is a “change hint” button that allows the user to write a textual hint, as suggested by the design partners from the co-design team.

securing access further by requiring physical objects, biometric input, and voice or handwriting analysis.

The most commonly explored alternatives are graphical passwords. For example, [5] investigates multiple types of graphical passwords. The research examined different kinds of graphical passwords, including their strengths and weaknesses. The article is reinforced by grounding the results of graphical password studies in research conducted on textual passwords. Comparisons between graphical and textual passwords lead to the largest gap in current research. Chiasson et. al [2] compared users’ retention of graphical passwords and textual passwords in adults using a graphical password system called PassPoints. In PassPoints, users select 5 points on an image and are required to click those 5 points to log in. The authors found that graphical passwords were easier to remember after the distraction task, but after “two weeks, recall of the passwords in the text and graphical conditions was not statistically different from each other” (p. 510).

Graphical passwords have been discussed as a viable alternative since 1999 in [9]. More recently, articles such as [3] showed the potential weakness of these passwords. The authors used computer models to identify and accurately predict users’ graphical passwords. Therefore the decision to investigate graphical passwords is not based on the assumption that graphical passwords are the ideal alternative. Instead, this study seeks to examine the strengths and weakness of one of the most prevalent alternative methods in children. This will hopefully identify the applicability of this method for children, leading to better login systems in the future.

What We Did

This study was performed to compare textual passwords, specifically the PassPoints-based system modified by an intergenerational design team and enabled graphical passwords for children. Researchers expected that a graphical password system would be more enjoyable and useful.

In the final password prototype developed for testing, participants created a text username then selected one of several images from a menu of images. They then selected five points on that image as their password. To access their account, the participant chose the same image and then selected the same five points in the same order. If they selected points that are within 20 pixels to their original selections, then they would successfully access their account.

A textual password interface was also created for empirical testing. This version of the site works exactly the same as the picture passwords except they created an alphanumeric password with the keyboard. Participants were prompted to create a hint which they can change at any point during the password confirmation process. Afterwards they were taken back to the home page and they could log in to their account by entering their username and their password.

When a participant completed each page (by successfully logging in to an account), the test moved to the next page based on the order set for that participant alternating randomly between graphical and textual pages.

Methods

Participants The study was completed with 13 participants between the ages of 6 and 12 years old (See Table 1). The study had a within-subjects design where all participants created textual and graphical passwords. Participants were randomly assigned to different orders for five different pages; some created textual passwords first

Name	*Age*	*Gender*
Archer	7	M
Caren	9	F
Marie	6	F
Xena	10	F
Kyle	9	M
Elizabeth	9	F
Alice	7	F
Mollys	10	F
Sally	9	F
Trent	12	M
Darren	8	M
Eric	6	M
Ian	8	M

Table 1: List of participants.

while others created graphical passwords first. All participants had some experience with passwords and login systems, but because of their young age, most did not have as extensive experience or as many different passwords as many adults. All of the children were from the Baltimore metropolitan region in the United States.

Protocol The study consisted of two lab-based session. The first session took approximately one hour and was completed by all 13 participants. The second sessions were held at least 10 days later and took approximately thirty minutes to complete. Participants used the same computer system and tried to recall the passwords that they had previously created.

First Session - Participants answered a few questions with the researchers and then created passwords for each of the five pages. They received a random order of graphical and textual passwords. All participants completed all five passwords. Each site was distinct and was identified by different colors, a different title, and a different logo image. After creating five accounts, participants were given approximately five minutes to play a game online as a distraction activity.

After completing the game, the children went back to try their passwords. If they failed to log in, they were given up to five attempts, but many children gave up after several unsuccessful attempts. They were encouraged to continue, but if they would not, they were given their password and advanced to the next page.

Once they attempted to log in to all five accounts, they were congratulated for their focus and hard work. They then answered a few questions about the process. These questions included questions about preference such as “What was easier to remember?” and “What did you prefer?” as well as questions about security in general, such as “Which of these would protect you better?”.

Second Session - Ten participants returned to the lab 11 to 16 days after they completed their first session. These participants tried to recall the passwords that they created previously.

Researchers observed as children moved through the process. After logging into the first page they then logged into the same five web site prototypes in the same order from the first session. If they could not log into a page, researchers provided the password for them and moved them to the next page. Once they completed the task, researchers asked them several questions about the experience. For example, they were asked if they felt their hints were useful, and if they felt graphical or textual passwords were more secure.

What We Found

The success rate is the number of successfully entered passwords divided by the total number of attempts. Table 2 shows the number of times participants attempted to access their account and the number of successfully entered passwords. A single attempt in this table can include multiple password entries, as long as the user continued to work on accessing their account.

It is clear from this table that participants did best during their first login. As soon as they were distracted for five minutes, they were much less successful at logging into their account. The success rate of graphical passwords dropped from approximately 87% to approximately 78%. The success rate of textual passwords dropped from a flawless 100% to approximately 81%. This implies that users forgot textual passwords more quickly, as the distraction task caused a greater difference with textual passwords than

		Attempts	*Successfully entries*	*Success Rate*
Graphical Passwords	Following account creation	33	29	87%
	After distraction task	33	26	78%
	After two weeks	26	11	42%
	Total	92	66	71%
Textual Passwords	Following account creation	32	32	100%
	After distraction task	32	26	81.25%
	After two weeks	24	16	66%
	Total	88	74	84%

Table 2: Success Rate of Passwords

graphical passwords (19% versus 9%). This implies that graphical passwords may be more memorable in the short term. But they were also more difficult for participants, as participants were able to access their accounts more consistently when using textual passwords.

What It Means

Even after two weeks most children did remember the generalities of their password. Most passwords were approximated, even when children couldn't access their accounts. They remembered what kinds of usernames and passwords they created, what picture they chose, and generally where the points were located on the image. Their troubles came from selecting specific locations, maintaining accuracy and order, and recalling the exact spelling, capitalization, and symbols following their passwords and usernames. This implies that both graphical and textual passwords are potentially viable, but concessions must be made to facilitate children. An alternative system may be able to capitalize on this knowledge to create a secure system that does not require the same specificity.

Limitations and Conclusion

Due to the lack of research in this area of Child-Computer Interaction, this study should be viewed as exploratory. As mentioned earlier, the field has thought about passwords, but the authors could not find any exploration of password solutions. This data is an excellent starting part, but further research could help strengthen the arguments of this paper and reveal better solutions.

This research had a small number of participants. Having only ten participants return for the second session was a disappointment. More participants were scheduled, but several canceled or forgot to show up to their second session.

It would be good to see more research on alternative graphical or picture password designs. This study showed that multi-point graphical passwords like PassPoints are problematic, but it also showed that children were able to remember objects and pictures with a great deal of accuracy. It would be interesting to study this further to discover the strengths and weakness of this capacity. It is likely that fertile new technologies could take advantage of this to create password systems that are both secure and child friendly.

Acknowledgments

The researchers would like to thank the University of Baltimore's Fund for Excellence, Google, the children and adults of KidsteamUB for helping with the prototype, and all of the participants.

References

[1] Attewell, P., Battle, J., and Suazo-Garcia, B. Computers and young children: Social benefit or social problem? *Social forces 82*, 1 (2003), 277–296.

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

[3] Devlin, M., Nurse, J. R., Hodges, D., Goldsmith, M., and Creese, S. Predicting graphical passwords. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, Springer (2015), 23–35.

[4] Dirik, A. E., Memon, N., and Birget, J.-C. Modeling user choice in the passpoints graphical password scheme. In *Proceedings of the 3rd symposium on Usable privacy and security*, ACM (2007), 20–28.

[5] Gołofit, K. Click passwords under investigation. In *European Symposium on Research in Computer Security*, Springer (2007), 343–358.

[6] Ives, B., Walsh, K. R., and Schneider, H. The domino effect of password reuse. *Communications of the ACM 47*, 4 (2004), 75–78.

[7] Mendori, T., Kubouchi, M., Okada, M., and Shimizu, A. Password input interface suitable for primary school children. In *Computers in Education, 2002. Proceedings. International Conference on*, IEEE (2002), 765–766.

[8] Read, J. C., and Cassidy, B. Designing textual password systems for children. In *Proceedings of the 11th International Conference on Interaction Design and Children*, ACM (2012), 200–203.

[9] Rubin, A. D., Jermyn, I., Mayer, A., Monrose, F., and Reiter, M. K. The design and analysis of graphical passwords. In *8th USENIX Security Symposium*, Citeseer (1999).

[10] Summers, W. C., and Bosworth, E. Password policy: the good, the bad, and the ugly. In *Proceedings of the winter international synposium on Information and communication technologies*, Trinity College Dublin (2004), 1–6.

[11] Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., and Memon, N. Authentication using graphical passwords: effects of tolerance and image choice. In *Proceedings of the 2005 symposium on Usable privacy and security*, ACM (2005), 1–12.

[12] Yarosh, S., Radu, I., Hunter, S., and Rosenbaum, E. Examining values: an analysis of nine years of idc research. In *Proceedings of the 10th International Conference on Interaction Design and Children*, ACM (2011), 136–144.