An Exploration of Graphical Password Authentication for Children

Hala Assal*, Ahsan Imran, Sonia Chiasson

Carleton University, Canada

Abstract

In this paper, we explore graphical passwords as a child-friendly alternative for user authentication. We evaluate the usability of three variants of the PassTiles graphical password scheme for children, and explore the similarities and differences in performance and preferences between children and adults while using these schemes. Children were most successful at recalling passwords containing images of distinct objects. Both children and adults prefer graphical passwords to their existing schemes, but password memorization strategies differ considerably between the two groups. Based on our findings, we provide recommendations for designing more child-friendly authentication schemes.

Keywords: Children authentication, Graphical passwords, Usability evaluation

1. Introduction

Children constitute a significant portion of Internet users; 99% of Canadian children aged 8 to 15 years are active online [1] and the statistics are similar in other countries [2]. Despite abundant authentication research, the literature on user authentication specifically for children is relatively sparse. In fact, the main focus of online security for children has been on designing methods for adults to protect their children [3, 4], or to

*Corresponding author

Email addresses: HalaAssal@scs.carleton.ca (Hala Assal), AhsanImran@cmail.carleton.ca (Ahsan Imran), chiasson@scs.carleton.ca (Sonia Chiasson)

[1]This project was supported by a grant from the Canadian Internet Registration Authority (CIRA)'s Community Investment Program.

educate children about the dangers of Internet usage [5].

Children do not necessarily have the same skills and preferences as adults, thus a child-oriented authentication system that better suits children's privacy and security needs is long overdue. In this paper, we seek to address the gap by exploring the usability of graphical passwords for children, and provide recommendations for developing authentication mechanisms for children that are more adaptable to their needs. We conducted two user studies with both children and adults in which they interacted with three graphical variants of the PassTiles [6] password scheme: Objects, Image, and Words PassTiles. We explore the similarities and differences in children's and adults' performance and perception. We found that *both* children and adults prefer graphical passwords to their existing schemes. This paper has the following contributions.

1. Attempts to address the gap of child-oriented user authentication by exploring the usability of graphical passwords for children.

2. Provides empirical results comparing children's and adults' performance and preferences while using three different graphical password schemes.

3. Provides recommendations for adapting user authentication for children.

Organization. Section 2 presents a background on user authentication. Section 3 presents the original PassTiles graphical password scheme and our adaptation. We present our user studies in Section 4, and the results in Section 5. The implications of the results and general recommendations for children's authentication are discussed in Section 6.

2. Background

2.1. Authentication

The most commonly used authentication schemes are knowledge-based [7, 8, 9], where the user memorizes a shared secret such as a password. Research has demonstrated that text-based passwords suffer considerabily from *both* security and usability issues [10, 9]. Bonneau *et al.* [9] developed a framework for evaluating alternative

authentication schemes based on usability, deployability, and security benefits. They found that no known scheme is ultimately better, suggesting that when choosing an alternative to text passwords, one needs to balance the advantages and tradeoffs, and choose the scheme that mostly fits one's needs.

2.2. Graphical Passwords

An extensive survey of the graphical password literature is provided by Biddle *et al.* [10]. We offer a brief summary of the most relevant issues here. Despite abundant authentication research, the literature on user authentication specifically for children is relatively sparse. We study graphical passwords [10] as an alternative authentication scheme for children. Psychology studies have acknowledged the human brain's superiority in recognizing and recalling visual information in contrast to textual information [11, 10]. Graphical passwords, a form of knowledge-based authentication, aim to utilize this human feature to reduce the user's cognitive load of memorizing passwords [12]. Graphical passwords can be categorized according to the cognitive task necessary to remember the password: recognition, recall, and cued recall [13]. Recognition is the least cognitively burdensome, where a user needs to decide whether the information presented to her matches what she had already memorized. Recall, on the the other end of the difficulty spectrum, requires the user to remember the information memorized without any clues. Cued recall offers some cues to trigger the user's stored memory [10, 12].

Several graphical password schemes have been proposed [10]. Some graphical passwords [14, 15] and related pattern-based schemes such as the Android screen unlock allow the user to choose their password, while others use system assigned passwords [16]. Draw-A-Secret (DAS) [14] allows users to draw their password on a grid, whereas, PassPoints [15] asks the user to choose five distinct click-points on an image presented by the scheme. Although allowing users to choose their passwords could be beneficial for usability, user studies of PassPoints found that different users tend to choose the same click-points, thus producing hotspots and reducing the password space [17]. Similarly, studies found that users tend to follow predictable patterns with pattern-based schemes [18]. PassFaces [16] assigns the user a system assigned password

of three faces that they need to distinguish from six distractor faces. In this paper, we use PassTiles [6], a graphical password system that uses system-assigned passwords for increased security. PassTiles was designed to allow comparison of the different types of memory retrieval. Our study focuses on two recognition based graphical passwords (Objects and Words PassTiles) and one cued recall graphical password (Image PassTiles) [6]. We discuss PassTiles in details in Section 3.

2.3. Children and Passwords

Recently researchers have taken interest in understanding how children perceive passwords to develop security guidelines and recommendations for children. Lorenz *et al.* [19] found that younger children were more receptive to security advice than teenagers and adults. Studies by Read *et al.* [20] and Coggins [21] investigated children's knowledge of text passwords. Both studies found that children, without any formal training, have at least some understanding of the purpose of passwords and how to create strong ones. On the other hand, Zhang-Kennedy *et. al.* [22] found that adults (parents and teachers) are primarily responsible for maintaining children's online credentials and the majority of children do not understand the reason why passwords should remain secret. Coggins recommends integrating the concept of computer passwords in elementary school curriculum, to teach children early on best practices of computer safety. He also suggests training children to memorize strings of random characters. Read *et al.* [23] recommend using analogies when explaining security concepts to children, e.g., keeping their game consoles safe in a drawer as an analogy to explain the importance of keeping their passwords safe.

2.4. Authentication for Children

Two US patents have been filed for relevant authentication schemes. Each took different approaches to authentication for children. Colella [4] proposed an authentication system that relies primarily on biometric identification. Using this authentication system, a third party Application Service Provider (ASP) assigns each child a "Safe Card" fingerprint scanner. The ASP maintains a database of approved websites for each child. To login, the child connects her Safe Card to her computer, performs local

authentication on it, and the card in turn opens the ASP's webpage and authenticates the child to the ASP. The child can then access any of the pre-approved websites through the ASP's webpage. M. Renaud and Mulji [24] proposed the "Little Bo Peep" scheme which guides users to create their own versions of familiar stories (e.g., fairy tales). Children can then use these stories as their authentication tokens. The authors claim that the personalization renders the stories more memorable than traditional authentication schemes.

On the adacemic side, K. Renaud [25] proposed an authentication system comprised of user-drawn icon-sized images (*Mikons* [26]) with password space equivalent to 15.9 *bits*. Renaud suggests its use for low-risk systems used by children. It was tested by children (11 and 12 years old) to access their online homework system. To sign up, each student drew four Mikons to represent their password, then the class teacher approved their choice of Mikons. To login, students choose their drawings from other distractor Mikons. They were presented with four sets of challenges, each containing 15 distractors and one of their Mikons. Over the period of 8 months, students logged into their homework system once every 2 months. Overall the system recorded an 87% success rate. However, this authentication scheme requires a human (the teacher in [25]) to verify the suitability of the Mikons, which is problematic for large-scale deployment. In addition, it did not perform well in terms of guessability; children were able to guess the creators of the Mikons when they were shown their classmates' drawings. Mendori *et al.* [27] designed a password system for grade 1 Japanese students, unfamiliar with the Roman alphabet and thus were unable to use traditional text passwords. Mendori's interface displays preset icons and symbols on a grid, and the child clicks on the ones that comprise their password. The researchers experimented with three different configurations, all with password space equivalent to 11.9 *bits*, however little has been published about the system's usability.

3. PassTiles

PassTiles [6] is a graphical password system designed to facilitate the comparison of different memory retrieval types by offering several configurable parameters. It presents

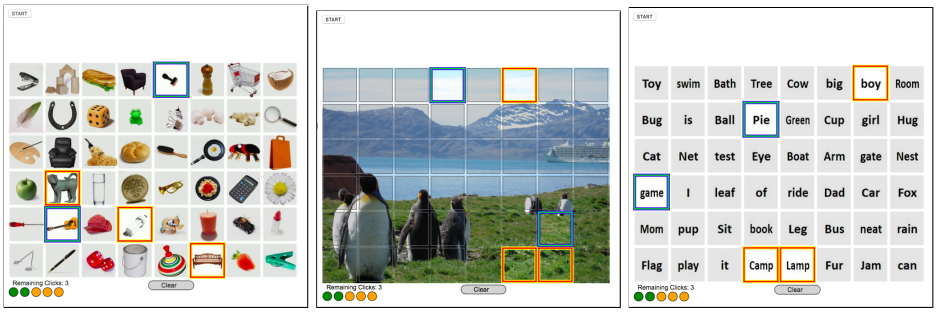
the user with a grid of tiles, and the password is composed of a subset of these tiles. The passwords are system assigned and generated through the Multiple Versatile Passwords (MVP) framework [28].

During the password memorization phase, the *password tiles* are visually highlighted with a coloured border. PassTiles users practice entering their password by clicking on the highlighted tiles in any order. When the user clicks a highlighted tile, the highlight colour changes to indicate selection. A visual, and numeric, counter is decremented with every click to show the number of tiles yet to be clicked. During login, the grid appears without highlighting, but the counter is displayed. To login, users click on their memorized tiles in no particular order.

We used three PassTiles schemes: Image, Objects, and Words. Each has 48 square tiles in a 6×8 grid, and each password is composed of 5 tiles. Image PassTiles [6] leverages cued recall by superimposing the tiles on a user-chosen background image,[2] which users can use as a cue to recall the location of their password tiles. Objects [6], and Words [29] PassTiles leverage recognition. Each tile in Objects PassTiles contains an image of an object, and the password is composed of a set of these objects. With each login, the tiles are shuffled, and users must rely on recognition to remember their password objects, rather than recalling the tile positions. Words PassTiles is similar to Objects, except it displays short simple words on the tiles.

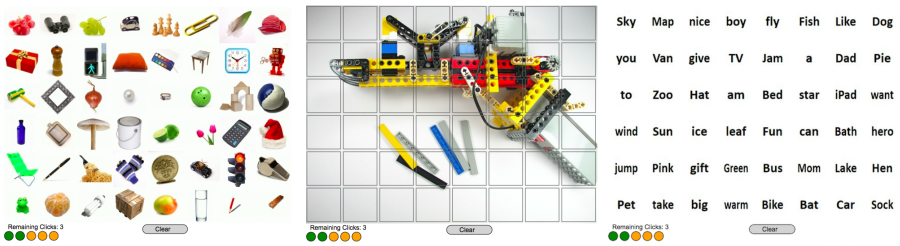
For the purpose of our study, we simplified the original PassTiles interface by removing non-essential features and simplifying the language to be better suited for children. We manually filtered the existing image set on MVP and added more age-appropriate images. Specifically, we filtered for items that children would readily recognize and would be able to name, such as, toys, fruits, and animals and items they might encounter in daily life. . For Words PassTiles, the existing set of words was modified to shorter and simpler ones. Figure 1 shows the three schemes during the memorization phase where 2 out of the 5 password tiles have been selected. The counter, at the bottom left of the screen, also shows that 3 tiles remain. Figure 2 shows the three schemes during the login phase. The interface does not highlight clicked tiles; in this

[2]The background image is user-chosen from a system-provided set.



(a) Objects PassTiles (b) Image PassTiles (c) Words PassTiles

Figure 1: Adapted PassTiles interface during memorization phase with highlighted password tiles. The orange highlight indicates the tile is yet to be clicked. A counter at the bottom left indicates the remaining number of tiles to be clicked (3 in this example).



(a) Objects PassTiles (b) Image PassTiles (c) Words PassTiles

Figure 2: Adapted PassTiles interface during login, where clicked tiles are not highlighted, but the counter is decremented.

example, the counter indicates that user has clicked two tiles.

3.1. Security of PassTiles

Knowledge-based authentication systems must be resilient against two main types of attacks: capture and guessing attacks [10]. Capture attacks involve acquiring the actual password or part thereof (e.g., using keyloggers or observing password entry through shoulder-surfing). A guessing attack is when the attacker tries to guess the password. Depending on circumstances, an attacker may be able to exhaustively search the theoretical password space (the total set of passwords an authentication scheme allows), guaranteeing success, or may be limited in the number of guesses. Using

knowledge of password distributions, an attacker can prioritize higher probability passwords (ones that users are more likely to use). Thus, to be resilient to guessing attacks, authentication systems should have an appropriately large theoretical password space and prevent predictable patterns in user-chosen passwords [10].

Recall, a PassTiles password is composed of 5 tiles on a grid of 6×8 tiles, and the order of password entry is insignificant. The size of the theoretical password space for PassTiles is $\log_2 \binom{\#rows \times \#columns}{password\ length} = \log_2 \binom{6 \times 8}{5} = 21\ bits$. Florêncio *et al.* [30] suggest that a password space of 20 bits is sufficient to protect against online guessing attacks. To reduce the success of guessing attacks, PassTiles uses system-generated passwords to utilize the full theoretical password space. In addition, system-assigned passwords protect against targeted guessing attacks, as users do not choose personally relevant elements. PassTiles does not highlight clicked tiles during password entry to reduce the risk of shoulder-surfing attacks.

4. Methodology

We conducted two user studies, one with children and one with adults. The adult study serves as our control condition. Our studies used a within subject design; each participant tested all three schemes (Objects, Image, and Words). For both studies, we used a balanced presentation order for the password schemes to minimize training effects. Both studies were reviewed and cleared by our institution's Research Ethics Board.

4.1. Procedure

Children Study. Each study session consisted of 5 phases, and lasted an average of 25 minutes. Each participant received a $10 gift card as compensation, even if they withdrew from the study.

Phase 1: Introduction and Consent

Consent The participants' parents signed a consent form agreeing to have their children participate in the study and be audio-recorded. The Children subsequently provided oral assent.

Introduction We explained to the participants the tasks they would be performing. We showed them printed snapshots of the three password schemes and explained verbally how the system worked and how they would enter their passwords once they were memorized.

Phase 2: Memorization and First login

Phase 2 was repeated three times, once for each password scheme. Participants completed Phase 2a followed by 2b for one scheme before moving to the next. They were given the chance to login only once for each scheme.

Phase 2(a): Memorize Password

Participants memorized the system-assigned password presented on the screen. Participants could practice entering their password as many times as they wanted. Once the participant had memorized the password, she was asked to click the start button.

Phase 2(b): First Login

On clicking the start button, participants were presented with the PassTiles interface with no highlighted tiles. Participants clicked on the tiles they thought composed their password, and the counter below the grid was incremented with every click. Once they had made five clicks, a popup box informed them if it was correct.

Phase 3: Interview

We interviewed participants to gather some insight about their preferences and perceptions of the three password schemes. The interview phase, which lasted for approximately 12 minutes, also served as a distraction period between the first and second login attempts (described in Phase 4). All interviews were audio recorded.

Phase 4: Second Login

To test memorability, participants were asked to perform a second attempt. The three schemes were presented to each participant in the same order as in the first login attempt, and each participant had only one attempt per scheme.

Table 1: Distribution of authentication schemes children have used on their tablets.

Authentication scheme	None	PINs	Passwords		Pattern
			alphanumeric	letters only	
Number of children	1	10	9	6	2

Adult Study. It followed the same procedure, with the following exceptions. The consent form was signed by the participants themselves, each participant received $10 compensation in cash, and each session lasted an average of 18 minutes.

4.2. Environment and Equipment

The children sessions took place either at our research labs or at a public library. Both offered a quiet, low-distraction environment. The adults sessions took place in our lab.

We used a Sony VAIO laptop with a touch-screen running Windows 8. Participants were instructed to use the mouse when interacting with PassTiles; however, three children found the mouse too difficult to use and switched to using the touchscreen.

4.3. Participant Demographics

4.3.1. Children Study

We recruited 25 children between 7 and 12 years of age ($mean = 9.5$ years), ten boys and fifteen girls. All children were accompanied by a parent. Twenty-four participants had previously used at least one type of authentication on their tablets. Table 1 shows the distribution of children's experience with existing authentication schemes. Twenty participants reported their parents taught them how to create passwords, two were taught by their older siblings, and two were self-taught.

4.3.2. Adult Study

We recruited 25 adults for this study. Twenty participants were between 18 and 30 years of age and five were over 30. Fourteen participants were male and eleven female. Five participants had a high school diploma, twelve had a Bachelor's degree, six had a Master's degree and two had Doctoral degrees. All participants were familiar with

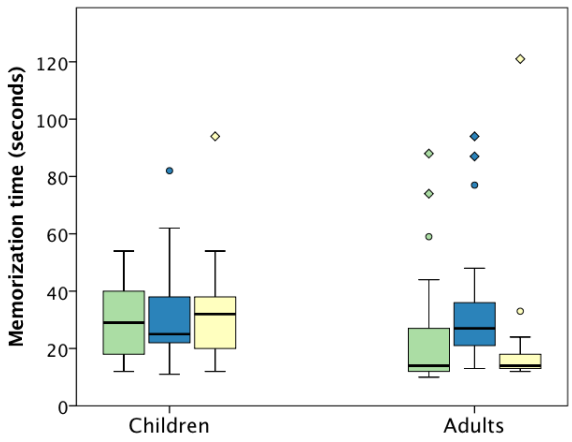


Figure 3: Memorization time for Objects, Image, and Words

the use of passwords and had experience using multiple passwords for different online accounts.

5. Results

We explored user performance through time and login success measures, and user preferences through interview questions.

We conducted Shapiro-Wilk test to check the normality of children's and adults' memorization and login times (first and second attempt) for the three schemes. The distribution of times significantly deviated from the normal distribution ($p < 0.05$), thus for these variables, we use non-parametric statistical tests.

For the following statistical tests, unless otherwise stated, we conduct Friedman tests to determine the differences between the three authentication schemes. In case of significant difference, we follow up using Bonferroni-corrected Wilcoxon post hoc tests. For these tests the calculated degrees of freedom is 2.

5.1. Memorization Time

We recorded the time spent memorizing each password, from the time the assigned password appeared until the participant clicked the start button to perform the first

login attempt. Figure 3 shows the descriptive statistics for the time spent by children and adults memorizing each scheme. Table 2 presents results of the statistical tests comparing times per scheme for the children and adults separately. Average times per scheme (in seconds) range from 29.5 to 32.6 for children and 20.1 to 33.5 for adults, with several outliers.

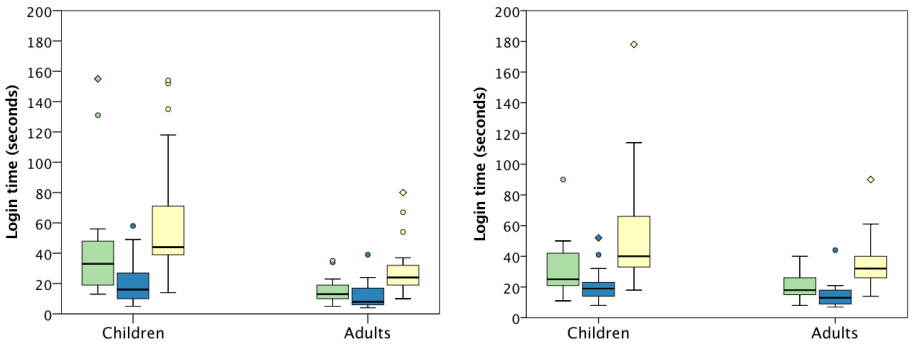
We found no statistical difference between schemes in children's memorization time. However, there was a statistical difference for adults; the post hoc test indicated that adults took significantly longer memorizing their Image password than the other two schemes. Since memorization time is a reflection of how much effort participants chose to devote to memorizing their password, we have no evidence that children perceived one scheme to be harder to memorize than the other, while evidence shows that adults perceived Image to be more difficult.

5.2. Login Times

The time spent entering each password was recorded, from the time participants clicked the start button until they clicked 5 tiles. Figure 4 shows the descriptive statistics for the time participants spent logging in using the three schemes. Table 2 presents results of the statistical tests measuring the effect of scheme for the first and second login attempts respectively, per study. Average login times (in seconds) range from 20.5 to 60.6 for children and 11.7 to 35.7 for adults, with much less variation for adults.

First Attempt. On the first attempt, children were significantly faster logging in using Image compared to the two other schemes. Children were also significantly faster logging in using Objects compared to Words. Similarly, login times for adults' first attempt were significantly different for the three schemes. The post hoc test shows that the login time for Words was significantly slower than that of Objects and Image. We conclude that on the first login attempt, children found Image the easiest to recall, followed by Objects, and both children and adults found Words the hardest scheme to recall.

Second Attempt. We found a statistical difference between children's second login times; the post hoc test shows that the login time for Words was statistically slower than



(a) First attempt (b) Second attempt

Figure 4: Time (*in second*) to login by children and by adults using Objects, Image, and Words

Table 2: Results from Friedman test and Bonferroni-corrected Wilcoxon post hoc test looking at differences between the three schemes in memorization and login times by children and by adults. The calculated degrees of freedom is 2.

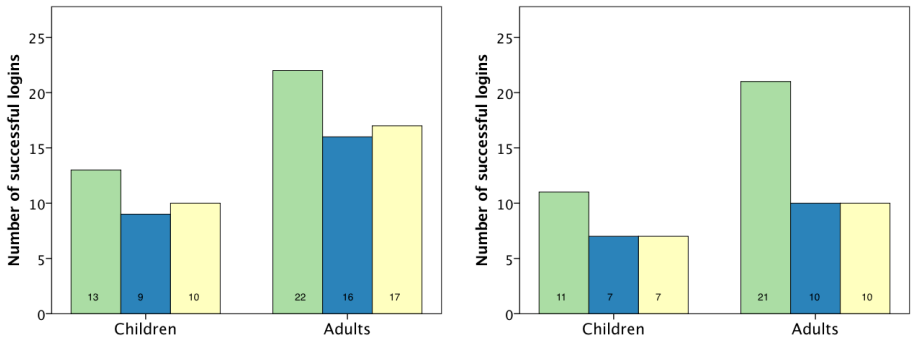
	Children					Adults				
	Friedman test		Post hoc			Friedman test		Post hoc		
time	X^2	p	O-I	O-W	I-W	X^2	p	O-I	O-W	I-W
Memorization	1.354	.508				17.111	.000	.006	1.000	.000
1^{st} login	30.081	.000	.007	.049	.000	22.566	.000	.537	.003	.000
2^{nd} login	29.714	.000	.071	.006	.000	26.929	.000	.022	.040	.000

O: Objects, I: Image, and W: Words. Colour indicates statistically significant results.

that of Objects and Image. Additionally, adults' second attempt login times for Words was statistically slower than Objects, which in turn was statistically slower than Image. We conclude that, on second attempt, adults found Image the easiest to recall, followed by Objects, and both children and adults found Words the hardest scheme to recall.

5.3. Login Success

We recorded whether each login was a successful or a failed attempt. Figure 5 shows the number of participants' successful logins. To test if there is a significant effect of scheme in each study, we use Cochran's Q test. We follow up on statistically significant results by conducting Bonferroni-corrected McNemar post hoc tests. The results of the statistical tests is presented in Table 3.



(a) First attempt

(b) Second attempt

Figure 5: Successful login attempts by children and by adults using Objects, Image, and Words

Table 3: Results from Cochran's Q test and Bonferroni-corrected McNemar post hoc test looking at difference in login success between the three schemes for children and for adults. The calculated degrees of freedom is 2.

	Children					Adults				
	Cochran's Q test		Post hoc			Cochran's Q test		Post hoc		
login success	X^2	p	O-I	O-W	I-W	X^2	p	O-I	O-W	I-W
1^{st} attempt	2	.368				4.133	.127			
2^{nd} attempt	2.909	.234				12.737	.002	.006	.006	1.000

O: Objects, I: Image, and W: Words. Colour indicates statistically significant results

First Attempt. On first attempt, we found no effect of scheme on login success for children or adults.

Second Attempt. There was no effect of scheme on login success for children's second attempt. However, we found statistical difference between the three schemes for adults. Adults were significantly more successful logging in using Objects than the other two schemes.

We built a logistic regression model to determine the effect of the length of memorization time on the likelihood that participants successfully logged in on the second attempt. However, the model was not significant, for neither children nor adults, thus memorization time cannot be used as a predictor for the outcome of the login attempt.

5.4. Degree of correctness

Compared to previous literature, adults' success rate is considerably lower. While no comparison is available for children and PassTiles, they also struggled with login. This could have been influenced by our study design, stressing memory by having three passwords memorized in a short time and allowing only one login attempt at a time. To explore further the reasons for low login success, we examined partially correct responses. We counted the number of correct tiles for each attempt. Figure 6 shows the descriptive statistics for the number of correctly chosen tiles.

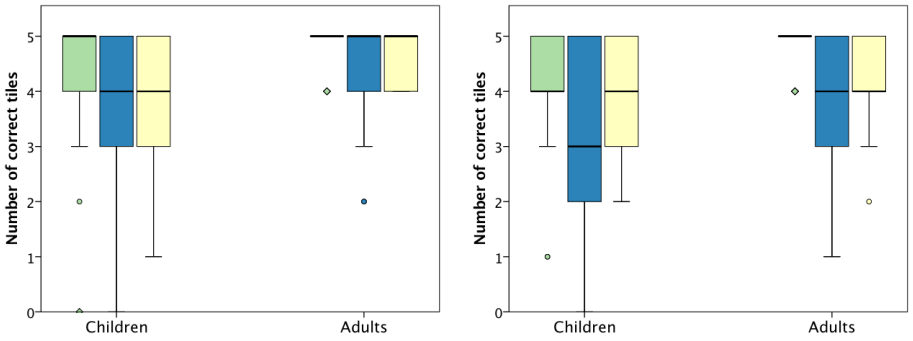
First Attempt. The median for each scheme is 4 or 5 correct tiles out of 5 on the first attempt, suggesting that participants had reasonable success at remembering most of their password. We found no effect of scheme on the degree of correctness for children, nor for adults.

Second Attempt. The degree of correctness for the second attempt showed more variability, particularly for the children. A Friedman test on the degree of correctness of children's second login attempt shows a statistical difference between the schemes, however, the pairwise comparison cannot identify with significant confidence which pairs differ. Looking at the data (see Figure 6b), we suspect that with a larger sample size, Objects would have the highest level of correctness while Image would be the worst. On the other hand, the degree of correctness for adults' second login attempt showed a statistical difference, and the post hoc test confirmed that adults' degree of correctness for Objects was significantly higher than that of Image and Words. We conclude that on second login attempt, adults found Objects the easiest to correctly recall, and children appear to be following the same trend.

5.5. Interview Results

We explored participants' perceptions and knowledge of online privacy and security, and asked them specific questions about the three schemes they tested; we asked participants:

- Which type of password did you like the most? *[Preferred scheme]*



(a) First login attempt

(b) Second login attempt

Figure 6: Number of correct tiles selected on each login attempt using Objects, Image, and Words

Table 4: Results from Friedman test and Bonferroni-corrected Wilcoxon post hoc test looking at differences between the three schemes in the number of correct tiles chosen by children and by adults. The calculated degrees of freedom is 2.

	Children					Adults				
	Friedman test		Post hoc			Friedman test		Post hoc		
correctness	X^2	p	O-I	O-W	I-W	X^2	p	O-I	O-W	I-W
1^{st} attempt	3.077	.215				4.978	.083			
2^{nd} attempt	6.200	.045	.198	.231	1.000	14.94	.001	.014	.022	1.000

O: Objects, I: Image, and W: Words

- Which one was the most difficult? *[Most Difficult scheme]*
- Which of the passwords do you think is the safest? *[Safest scheme]*

For each question, we tabulated the number of participants that identified a scheme in their response. Figure 7 summarizes participants' responses. The Safest scheme question has only 24 responses; one child could not identify the safest scheme. We conducted One-Way Chi Square tests to determine whether a scheme stood out as the most preferred, the most difficult, the safest, by comparing to expected even distributions of 8.5 responses per scheme.

5.5.1. Preferred Scheme

We did not find statistical evidence of one scheme being more preferred by children ($X^2(2, N = 25) = 2.960, p = 0.228$), nor by adults ($X^2(2, N = 25) = 1.520, p = 0.468$). Looking at the distributions in Figure 7, we see very similar patterns between children and adults; Objects was the preferred scheme for 48% of the children and 44% of adults, followed by Words then Image. A larger sample would be needed to confirm this trend.

5.5.2. Most Difficult Scheme

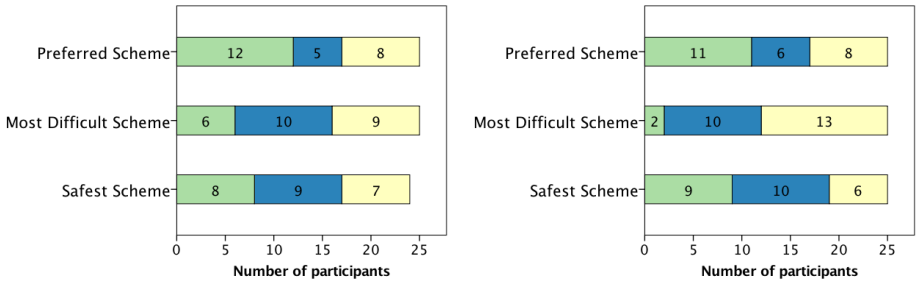
We found no statistical evidence of one scheme being perceived by children as the most difficult ($X^2(2, N = 25) = 1.040, p = 0.595$). However, adults perceived Objects to be the least difficult ($X^2(2, N = 25) = 7.760, p < 0.05$). This coincides with it being preferred by more adults compared to Objects and Image.

5.5.3. Safest Scheme

We asked the participants which password scheme they thought was the safest and the most difficult to guess or hack. Figure 7 shows a very similar pattern between children and adults, in terms of their perceived safety of the schemes, and no significant effect of scheme was found for both children ($X^2(2, N = 25) = 0.250, p = 0.882$) and adults ($X^2(2, N = 25) = 1.040, p = 0.595$).

5.5.4. Understanding of Security

We found that compared to children, adults have a much better understanding of online privacy and security, and they reported well-known security advice, such as, not



(a) Children (b) Adults

Figure 7: Interview Results showing the number of participants choosing Objects, Image, and Words

sharing passwords with others, frequently changing passwords, and avoiding logging in to untrusted websites. On the other hand, only a small number of children reported any advice. Among those who did, they explained that they should not share their passwords with anyone and should not give their personal information to strangers, they should have strong passwords stored in a safe place, and they should not click on ads or give their email addresses to strangers. The majority of children rely on their parents for managing their passwords; they either share their passwords with their parents, or they ask their parents to reset their passwords for them if they have trouble remembering them. Only six children manage their passwords on their own, and they reported writing them down. We found, contrary to previous research [20, 21], that the majority of children are fairly unaware of security practices and may be particularly vulnerable to attacks.

5.5.5. Observations

While using the adapted PassTiles interface, three children found it difficult to use the mouse and opted to use the touchscreen for inputting their passwords. All in all, children did not show any signs of confusion using the interface and were able to perform the tasks without major problems. The adults similarly did not encounter any significant hurdles.

However, we observed that *both* children and adults made the mistake of clicking the same tile twice during login, without noticing the number-of-clicks counter. This

happened by either double-clicking a tile (rather than a single click) or by forgetting the tile was clicked, and clicking it again. Clicked tiles are not highlighted during the login phase to help protect users from shoulder surfing attacks.

Additionally, the two youngest participants (7 years old) had trouble pronouncing the Words password, making it difficult for them to identify their tiles. On the other hand, several adult participants and the older child participants tried to memorize the Words and Objects password by forming a sentence with the words, or the objects' names.

Finally, we observed that children were generally interested in the study and were keen on learning how the passwords worked. However, they overlooked the pop-up message notifying them whether their login attempt was successful. This feedback, which was intended to help with the formation of a correct mental model of the system, was noticed by almost all adult participants but ignored by the majority of the children.

6. Discussion

The majority of children learned about passwords from their parents or older siblings. However, advice they receive from adults is not necessarily ideal; adults struggle with passwords and they do not always follow security best practices, which even applies to security experts [31] and system administrators [32]. Moreover, coping strategies that adults use are not necessarily applicable or useful for children. For example, to easily memorize the Words password, some of the adults formed a sentence with the words appearing on the highlighted tiles. However, we observed that children were struggling with this scheme; they took the longest logging in using Words and they had much trouble memorizing their Words password. Therefore, when designing authentication systems for children, we especially need to think about their skills, cognitive abilities, and preferences, since these can have significant impact on children's ability to use the system.

We found that, when choosing an image for Image PassTiles, most adults chose an image they thought would be most helpful in remembering—having a variety of content in different locations. On the other hand, children selected images they found

to be interesting, usually containing animals or toys, and ignoring whether it would be easy to remember when divided into tiles. Cued recall works best with unique cues on the background image, and since children are inattentive to this fact, it is important that the pool of images for Image PassTiles should have enough distinct features to help with memorability. In addition, if we allow users to upload their own images, as suggested by some of the children participating in our study, these images should undergo a prescreening process to make sure they are feature-rich. For example, if a user uploads an image of the sea, where only the sea and the sky are visible in the image, then all the tiles on the image will look similar. In this case, rather than remembering her password by recognizing image features, the user will need to remember the locations of her password tiles without any useful image cues. Image processing techniques exist to identify and extract features from images. With graphical passwords, there is some literature on automatically identifying "clickable points" within images, either for helping select appropriate images or for helping automate attacks [33, 34].

During the memorization phase, adults generally did not practice entering their passwords as often as children did; they spent the time observing the password carefully. However, adults perceived Image PassTiles to be harder to memorize, so they spent significantly more time memorizing it than the other two schemes. On the other hand, children took their time to memorize their passwords and practiced them several times before logging in. However, despite practicing, children had trouble remembering their passwords. Perhaps because adults are more familiar with the process of learning passwords than children, they may have been better able to draw on these past experiences to come up with successful memorization strategies. On designing passwords for children, we may need to offer additional support to guide their memorization efforts, *e.g.,* it might be possible to extend password memorization through gamification to achieve better success.

Children's reliance on their parents to maintain login credentials may have denied them the opportunity to devise appropriate password memorization strategies. However, we do not expect children, many of whom are still learning reading and writing skills, to be able to memorize strong text passwords. Since graphical passwords provide comparable security benefits and do not require literacy, they could be a plausible

alternative that allows children to manage their credentials independently.

Although the login success rates in our study were much lower than would be necessary for a real world deployment, this could be due to the study structure. The scenario was more difficult than would be in a real life situation, *e.g.,* users do not normally have to memorize three different passwords in a very short timeframe. Thus, in the real world, we would expect the login success rates to increase. However, we can see this is an especially hard task for children. In a later study, Cole et al. [35] explored PassPoints in a study with similar methodology to ours. Although children generally recalled aspects of their passwords, they similarly found that children had difficulty remembering specific details of both graphical and text-based passwords. Based on these experiences and observations, we make the following recommendations for children's authentication.

R1. Facilitate memorization through learning and training features

Password memorization is a challenging cognitive task in general and systems using password authentication should support the process of memorizing secure passwords. User-chosen passwords might be easier to memorize than system assigned passwords, however, allowing users to choose their own graphical passwords might reduce security benefits. Previous research [33, 34] found that user-chosen graphical passwords are usually weak (*e.g.*, users tend to chose corner tiles, or familiar objects). For example, children may tend to choose objects containing images of popular toys or their favourite ones, which would make them more vulnerable against guessing attacks. Thus, it is especially important to support the process of password memorization.

We recommend incorporating learning/training features to facilitate memorization within the password creation process. Due to children's inattentiveness to system notifications, and because interactive training features might prove to be more successful for children [36], we would recommend a more attractive method of notification that includes positive feedback from the system as encouragement. We would also like to encourage the creation of stories during the memorization process of both Objects and Words PassTiles by linking together the password's words or objects and incorporating this strategy into the user interface.

R2. Adapt interface to be age-appropriate for children

We observed age-related differences in how children memorized their passwords and interacted with the interface. As with earlier research [37], our work indicates that we need different computer interfaces for children throughout the stages of development. For example, for younger children, we could use colourful words from age appropriate curriculum or from popular storybooks in Words PassTiles, and familiar objects such as animals and toys in Objects PassTiles. To help with their interaction with graphical passwords, we recommend using touchscreen input instead of mouse input as children tend to accidentally drag and double-click [37] with the mouse which could lead to false input. Additionally, it might be useful, for children as well as adults, to refrain from counting duplicate clicks on the same tile towards the total count of inputed password tiles.

Although participants had less than desirable login success rates, looking more closely we see that most participants had nearly correct entries. This may indicate that shorter passwords might be more manageable for children (albeit at a decrease in security). Alternatively, a system which accepts entries as correct if they meet a certain threshold may also be conceivable, which aligns with Chatterjee *et al.*'s [38] typo-tolerant password authentication framework, and Cole et al.'s findings [35] about children remembering generalities.

R3. Combine schemes to improve memorability

We were surprised that adults found Words PassTiles to be the most difficult scheme. We had assumed that because adults have a bigger vocabulary and are more experienced with words, they would find Words PassTiles more favourable. Although children generally had difficulty, the ones who formed stories with the words in their passwords remembered them better. We recommend using words with pictures to provide additional cues that could help with memorization. This could also be beneficial in circumstances where a user does not recognize the object illustrated.

In addition to being an alternative to text passwords, graphical passwords can be used to teach children about passwords and authentication in general. In our study, as children interacted with the interface, they became more inquisitive about the schemes.

Graphical password interfaces centre on visual elements, which may provide a more enjoyable and engaging learning setting for children. Using graphical passwords as a learning tool, especially using multitouch screens, would seem like playing a game, rather than learning a lesson.

7. Limitations and Future Work

Our study has the following limitations. In this study, authentication was participants' primary task. This does not necessarily reflect real life scenarios, where users would need to enter their passwords to perform their primary task (*e.g.*, play games or check their email). In addition, the study lasted for one hour, a longer time span is needed to study password memorability. We acknowledge that these limitations might have affected the results of our study. Our study was useful for comparing differences between the three schemes. Long-term memorability of the more promising schemes should be tested with a multi-session study over several weeks or months.

In future studies, we will collect more qualitative data to investigate strategies that children use to create and memorize their passwords, as well as factors that could influence a password's memorability (*e.g.*, are certain types of pictures easier to memorize than others?). We will also further investigate failed logins by looking at environmental factors that might lead users to err while entering their password (do children make more errors when it is noisy? and and exploring the types of errors made (are the incorrect tiles usually at the beginning, or the end of the password?).

We will also explore factors leading adults to be more successful than children in using the schemes: are adults more successful because they have previous experience with passwords? What strategies do adults use to memorize passwords? And can children benefit from these strategies?

8. Conclusion

Despite the abundance of work looking at authentication mechanisms, the literature addressing children's authentication is relatively sparse. We explored graphical

passwords as an alternative authentication method for children through two user studies—one with children and another with adults. Both children and adults preferred graphical passwords to their existing authentication scheme. Of the three schemes, children were most successful with Objects PassTiles, although they had some difficulty completely recalling any of their passwords. We explored similarities and differences in preferences and performance between children and adults. For example, we found that children are less careful when memorizing their passwords than adults and memorization strategies that adults use are not always applicable for children. Thus, it is necessary to consider children's cognitive abilities and skills to design child-friendly authentication systems.

References

[1] V. Steeves, Young Canadians in a Wired World, Phase III: Life Online, http://mediasmarts.ca/sites/mediasmarts/files/pdfs/publication-report/full/YCWWIII_Life_Online_FullReport.pdf, [Accessed August-2016] (2014).

[2] D. Holloway, L. Green, S. Livingstone, Zero to eight: Young children and their internet use.

[3] K. Channakeshava, K. Bian, M. S. Hsiao, J.-M. Park, R. E. Crossler, F. Bélanger, P. Aggarwal, J. S. Hiller, On Providing Automatic Parental Consent over Information Collection from Children, in: Security and Management, 2008, pp. 196–202.

[4] B. Colella, System for secure internet access for children, US Patent 7,853,535 (Dec. 14 2010).
URL https://www.google.com/patents/US7853535

[5] J. A. Rode, Digital Parenting: Designing Children's Safety, in: Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology, BCS-HCI '09, British Computer Society, Swinton, UK, UK, 2009, pp. 244–251.
URL http://dl.acm.org/citation.cfm?id=1671011.1671041

[6] E. Stobert, R. Biddle, Visual end-user security, in: VL/HCC, 2012, pp. 233–234.

[7] W. Stallings, M. D. Bauer, M. Howard, L. Brown, Computer Security: Principles and Practice, Prentice Hall, Upper Saddle River, N.J, 2008.

[8] B. Schneier, Sensible Authentication, Queue 1 (10) (2004) 74–78. doi:10.1145/971564.971595.
URL http://doi.acm.org/10.1145/971564.971595

[9] J. Bonneau, C. Herley, P. C. v. Oorschot, F. Stajano, The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes, in: Security and Privacy (SP), 2012 IEEE Symposium on, 2012, pp. 553–567. doi:10.1109/SP.2012.44.

[10] R. Biddle, S. Chiasson, P. Van Oorschot, Graphical Passwords: Learning from the First Twelve Years, ACM Comput. Surv. 44 (4) (2012) 19:1–19:41. doi:10.1145/2333112.2333114.
URL http://doi.acm.org/10.1145/2333112.2333114

[11] E. A. Kirkpatrick, An experimental study of memory, Psychological Review 1 (6) (1894) 602.

[12] S. Chiasson, P. C. Oorschot, R. Biddle, Graphical Password Authentication Using Cued Click Points, in: Computer Security – ESORICS 2007: 12th European Symposium On Research In Computer Security, Dresden, Germany, September 24 — 26, 2007. Proceedings, Springer Berlin Heidelberg, Berlin, Heidelberg, 2007, pp. 359–374. doi:10.1007/978-3-540-74835-9_24.
URL http://dx.doi.org/10.1007/978-3-540-74835-9_24

[13] J. Raaijmakers, R. Shiffrin, Models for recall and recognition, Annual Review of Psychology 43 (1992) 205–234.

[14] I. Jermyn, A. J. Mayer, F. Monrose, M. K. Reiter, A. D. Rubin, et al., The design and analysis of graphical passwords., in: Usenix Security, 1999, pp. 1–14.

[15] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, N. Memon, Passpoints: Design and longitudinal evaluation of a graphical password system, International journal of human-computer studies 63 (1) (2005) 102–127.

[16] R. U. P. Authentication, The science behind passfaces, White Paper, June.

[17] S. Chiasson, R. Biddle, P. C. van Oorschot, A second look at the usability of click-based graphical passwords, in: Proceedings of the 3rd symposium on Usable privacy and security, ACM, 2007, pp. 1–12.

[18] S. Uellenbeck, M. Dürmuth, C. Wolf, T. Holz, Quantifying the security of graphical passwords: the case of android unlock patterns, in: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, ACM, 2013, pp. 161–172.

[19] B. Lorenz, K. Kikkas, A. Klooster, "The Four Most-Used Passwords Are Love, Sex, Secret, and God": Password Security and Training in Different User Groups, in: Human Aspects of Information Security, Privacy, and Trust: First International Conference, HAS 2013, Held as Part of HCI International 2013, Las Vegas, NV, USA, July 21-26, 2013. Proceedings, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, pp. 276–283. doi:10.1007/978-3-642-39345-7_29.
URL http://dx.doi.org/10.1007/978-3-642-39345-7_29

[20] J. C. Read, B. Cassidy, Designing Textual Password Systems for Children, in: Proceedings of the 11th International Conference on Interaction Design and Children, IDC '12, ACM, New York, NY, USA, 2012, pp. 200–203. doi:10.1145/2307096.2307125.
URL http://doi.acm.org/10.1145/2307096.2307125

[21] P. E. C. III, Implications of What Children Know About Computer Passwords, Computers in the Schools 30 (3) (2013) 282–293. arXiv:http://dx.doi.org/10.1080/07380569.2013.807719, doi:10.1080/07380569.2013.807719.
URL http://dx.doi.org/10.1080/07380569.2013.807719

[22] L. Zhang-Kennedy, C. Mekhail, Y. Abdelaziz, S. Chiasson, From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats, in: Interaction Design and Children (IDC), ACM, 2016.

[23] J. C. Read, R. Beale, Under My Pillow: Designing Security for Children's Special Things, in: Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology, BCS-HCI '09, British Computer Society, Swinton, UK, UK, 2009, pp. 288–292.
URL http://dl.acm.org/citation.cfm?id=1671011.1671046

[24] M. Renaud, R. Mulji, Authentication system, such as an authentication system for children and teenagers, US Patent App. 11/693,438 (Nov. 8 2007).
URL https://www.google.com/patents/US20070261109

[25] K. Renaud, Web Authentication Using Mikon Images, in: Privacy, Security, Trust and the Management of e-Business, 2009. CONGRESS '09. World Congress on, 2009, pp. 79–88. doi:10.1109/CONGRESS.2009.10.

[26] Mikons.com: Create and Connect, http://www.mikons.com, [Accessed February-2016].

[27] T. Mendori, M. Kubouchi, M. Okada, A. Shimizu, Password input interface suitable for primary school children, in: Computers in Education, 2002. Proceedings. International Conference on, 2002, pp. 765–766 vol.1. doi:10.1109/CIE.2002.1186069.

[28] S. Chiasson, C. Deschamps, E. Stobert, M. Hlywa, B. Freitas Machado, A. Forget, N. Wright, G. Chan, R. Biddle, The MVP Web-Based Authentication Framework, in: Financial Cryptography and Data Security: 16th International Conference, FC 2012, Kralendijk, Bonaire, Februray 27-March 2, 2012, Revised Selected Papers, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012, pp. 16–24. doi:10.1007/978-3-642-32946-3_2.
URL http://dx.doi.org/10.1007/978-3-642-32946-3_2

[29] N. Wright, A. S. Patrick, R. Biddle, Do You See Your Password?: Applying Recognition to Textual Passwords, in: Proceedings of the Eighth Symposium on Usable Privacy and Security, SOUPS '12, ACM, New York, NY, USA, 2012, pp. 8:1–8:14. doi:10.1145/2335356.2335367.
URL http://doi.acm.org/10.1145/2335356.2335367

[30] D. Florêncio, C. Herley, P. C. van Oorschot, An Administrator's Guide to Internet Password Research, in: 28th Large Installation System Administration Conference (LISA14), USENIX Association, Seattle, WA, 2014, pp. 44–61.
URL https://www.usenix.org/conference/lisa14/conference-program/presentation/florencio

[31] E. Stobert, R. Biddle, Expert Password Management, in: Technology and Practice of Passwords: 9th International Conference, PASSWORDS 2015, Cambridge, UK, December 7-9, 2015, Proceedings, Springer International Publishing, Cham, 2016, pp. 3–20. doi:10.1007/978-3-319-29938-9_1.
URL http://dx.doi.org/10.1007/978-3-319-29938-9_1

[32] A. Abdou, D. Barrera, P. C. van Oorschot, What Lies Beneath? Analyzing Automated SSH Bruteforce Attacks, in: Technology and Practice of Passwords: 9th International Conference, PASSWORDS 2015, Cambridge, UK, December 7-9, 2015, Proceedings, Springer International Publishing, Cham, 2016, pp. 72–91. doi:10.1007/978-3-319-29938-9_6.
URL http://dx.doi.org/10.1007/978-3-319-29938-9_6

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

[34] J. Thorpe, P. C. van Oorschot, Human-seeded attacks and exploiting hot-spots in graphical passwords., in: USENIX Security, Vol. 7, 2007.

[35] J. Cole, G. Walsh, Z. Pease, Click to enter: Comparing graphical and textual passwords for children, in: Conference on Interaction Design and Children (IDC), ACM, 2017, pp. 472–477. doi:10.1145/3078072.3084311.

[36] A. N. Antle, LIFELONG INTERACTIONS: Embodied Child Computer Interaction: Why Embodiment Matters, interactions 16 (2) (2009) 27–30. doi:10.1145/1487632.1487639.
URL http://doi.acm.org/10.1145/1487632.1487639

[37] A. Bruckman, A. Bandlow, A. Forte, HCI for kids (2002).

[38] R. Chatterjee, A. Athalye, D. Akhawe, A. Juels, T. Ristenpart, pASSWORD tYPOS and How to Correct Them Securely, in: 37th IEEE Symposium on Security and Privacy, 2016.