IMPROVING CHILDREN'S AUTHENTICATION PRACTICES WITH RESPECT TO GRAPHICAL AUTHENTICATION MECHANISM

by
Dhanush Kumar Ratakonda

A dissertation

submitted in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy in Computing

Boise State University

August 2022

BOISE STATE UNIVERSITY GRADUATE COLLEGE

DEFENSE COMMITTEE AND FINAL READING APPROVALS

of the dissertation submitted by

Dhanush Kumar Ratakonda

Dissertation Title: Improving Children's Authentication Practices with Respect to Graphical Authentication Mechanism

Date of Final Oral Examination: 22 April 2022

The following individuals read and discussed the dissertation submitted by student Dhanush Kumar Ratakonda, and they evaluated the presentation and response to questions during the final oral examination. They found that the student passed the final oral examination.

Jerry Alan Fails, Ph.D.	Chair, Supervisory Committee
Maria Soledad Pera, Ph.D.	Member, Supervisory Committee
Hoda Mehrpouyan, Ph.D.	Member, Supervisory Committee

The final reading approval of the dissertation was granted by Jerry Alan Fails, Ph.D., Chair of the Supervisory Committee. The dissertation was approved by the Graduate College.

ACKNOWLEDGEMENTS

This dissertation work would not be possible without several people in my life and Ph.D. journey. First and foremost, I sincerely thank my mom Kavitha Malepati, and my dad Sudarshan kumar Ratakonda, for their support in every way possible. I thank my lovely wife, Meghana Endluri, for being an excellent partner, by all means, especially listening and having discussions with all the ideas I came up with during this work. Thank you Mahesh Kurapati, Sunitha Kurapati, and Manoj Kurapati, for your extreme support since my childhood.

In my opinion, a genuine human being cares both professionally and personally about his surrounded people. Dr. Jerry Alan Fails is a genuine human being who was extremely helpful to me as I navigated my Ph.D. His insights are invaluable, and his empathy towards his students is unbeatable. Dr. Jerry Alan Fails, thank you so much for everything. The suggestions from my Committee members, Dr. Maria Soledad Pera and Dr. Hoda Mehrpouyan, strengthened, sharpened, and refined the research. I thank Dr. Maria Soledad Pera and Dr. Hoda Mehrpouyan for their expert insights and guiding me through this dissertation work.

I am very glad that I had a roommate who is one of my best friends Dr. Shivakumar Rayavara Veerabhadraiah, thank you for always being open to listening and

giving me advice about my career and life. Shiv, your suggestions were invaluable and have made me a better human being. I also would like to mention my other best friends, Akhil, Manikanta, Prem, Pavan, Rahul, Venkat, Viswas, for being supportive and helping me in this journey.

Last but not least, I want to extend my gratitude to all Kidsteam kids and parents for helping to achieve this research work. Thanks to children and their parents who participated in multiple studies through out this work. My sincere thanks to Elizabeth Barnes for help in recruiting children for some of this work.

ABSTRACT

A variety of authentication mechanisms are used for online applications to protect user's data. Prior literature identifies that adults and children often utilize weak authentication practices and our own initial research corroborates that children often create weak usernames and passwords. One reason children adopt weak authentication practices is due to difficulties in remembering their usernames and passwords. Existing literature suggests that people are better at remembering graphical information than text and words. In this dissertation, my research goal is to improve the **usability** and **security** of **children's authentication mechanisms**. My research includes designing, developing, and evaluating a new graphical user authentication mechanism for children where children choose a sequence of pictures as their password. In our studies, this mechanism, named *KidsPic*, allowed children (ages 6-11) to create and remember their passwords better than an alphanumeric password.

Usability studies identified areas needing further investigation with regards to usability and security. With regards to *usability*: we investigated whether resolution influences picture selection, the influence of category order on memorability, if the number of objects in a picture influences its selection, and if picture features like dominant colors influences picture selection. With regards to *security*: we designed and implemented mechanisms to mitigate brute-force and shoulder surfing attacks. For guessing attacks, we conducted a usability study with child dyads. The results

and analysis from these additional usability research objectives revealed no influence of picture resolution, order of picture categories, number of objects in each picture, and dominant colors on children choosing pictures for their password. The security research objectives resulted in design enhancements of KidsPic that mitigate brute-force, shoulder surfing, and guessing attacks.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

IDC – Interaction Design and Children

IRB – Institutional Review Board

BSU – Boise State University

HCI – Human Computer Interaction

PHP – PHP HyperText Preprocessor

RDBMS – Relational Database Management System

UI – User Interface

SQL – Structured Query Language

URL – Uniform Resource Locator

PII – Personal Identifiable Information

CHAPTER 1

INTRODUCTION AND MOTIVATION

The increasing use of technology requires users to create more online accounts, each of which usually require a form of authentication (username and password). Children are also increasingly using technology for school and leisure activities and, as such, often create online accounts that require them to utilize authentication mechanisms. Authentication poses many challenges for adults and several additional challenges for children. Though there are many rules in place to regulate children's data such as the General Data Protection Regulation (GDPR) and Children's Online Privacy Protection Act (COPPA), online security/data breaches are increasing day-by-day around the world and are increasingly targeting children [2]. These breaches target users' personally identifiable information (PII). Among many reasons for online security breaches, the one primary reason is using weak authentication practices [3]. Good authentication practices include creating passwords with different combinations of symbols and numbers, using longer passwords, and not including PII as part of their passwords to secure their online accounts – in order to make it harder for someone else to guess or *hack* their password [4].

In this dissertation, my entire research work is focused to address the following primary research questions: (1) What are children's current authentication practices,

and (2) Can children's authentication practices be improved in terms of security and usability through a graphical authentication mechanism?

Research conducted to understand children's authentication practices revealed that children have a theoretical understanding about creating and using passwords. However, traditional alphanumeric mechanisms pose memorability issues which lead children not to follow the best practices [5, 6, 7, 8, 9]. After completing an in-depth literature review about children's authentication practices, as a first step in my research, I sought to better understand children's authentication practices with regards to various authentication practices. In particular how elementary school children (ages 5-11) create and use usernames and passwords. Since parents and teachers can have an influence with regards to how children access online systems, we also surveyed adults in these roles as to their: (1) own understanding and practices with regard to authentication, and (2) perceptions of how children understand and utilize authentication mechanisms. To investigate these two populations, we conducted semi-structured interviews with children, and an online survey for parents and teachers. The semi-structured interviews with children consisted of questions relating to ten security dimensions which were not collectively studied in a single study in the literature. We grouped all the security dimensions into three larger security categories for credentials including: (1) composition (security strength, self related); (2) performance (memorability, error rate, time to enter, over the shoulder); and, (3) mechanisms (usage in schools, reuse, preference, and administration). The online survey for adult participants asked a set of questions which also addressed the security dimensions above. The combination of children and adult perspectives along with the breadth of authentication dimensions explored and analyzed led us

to determine the need to develop an authentication mechanism for children which helps their memorability and maintains security. This research was published in the Interaction Design and Children (IDC) 2019 Conference [6].

A few studies have attempted to compare alternative password mechanisms (graphical authentication mechanism) for children. For example, a study found that children have memorability issues with the PassPoints (a recall-based) authentication mechanism remembering the exact click-points as their password [10]. A few psychology studies revealed that humans can better remember visual information better than textual based information [11, 12, 13, 14, 15], as the second step of this research work, I sought to develop an graphical-based authentication mechanism which I further evaluate for usability and security. To achieve this goal, we conducted a series of formative studies to better understand children's memorability issues and their preference between alphanumeric (recall-based) and graphical authentication mechanisms (recognition-based). The collected data from formative studies suggested that children are good at remembering graphical passwords when compared to their alphanumeric passwords. These studies were used to inform design work that used the *Cooperative Inquiry* method [16, 17] where an intergenerational design team worked to design a graphical password mechanism that matches the theoretical password space of typical alphanumeric password where typically eight characters are required. The result of this design work is the "KidsPic" authentication mechanism. In efforts to increase the security of KidsPic, we enhanced the theoretical password space of the KidsPic authentication mechanism. The detailed explanation regarding how we increased the theoretical password space is in Chapter 5. In the enhanced KidsPic authentication mechanism, children select seven pictures in a series of categories to

make their picture password. We conducted usability studies with child participants (ages: 6-11, n = 40, mean age: 8.5) to understand the usability and memorability (using primarily the total number of failed login attempts) of enhanced picture password (KidsPic) and a traditional alphanumeric authentication mechanism.

Though the results from the usability study informed us that KidsPic improved memorability, we observed that there are a few instances where the same picture was selected by child participants in all the picture categories – which means that they are not using the entire theoretical password space of KidsPic. To further understand the child participant's picture selection behavior, we structured a few research objectives (RO1-7) from Chapter 6 that helped us understand their picture selection preferences. Subsequently, further advances to KidsPic would avoid the brute-force attack, shoulder surfing attack, and guessing attacks.

In order to address my primary research questions of understanding (Chapters 2, 3)and improving (Chapters 4, 5, 6) children authentication practices this dissertation progresses as follows: Chapter 2 contains a review and synthesis of research related to children's authentication practices. Chapter 3 describes the studies conducted to understand children authentication practices related to alphanumeric, pattern, and numeric-based authentication mechanisms. Chapter 4 describes the methods utilized to design and evaluate the usability of KidsPic authentication by measuring memorability using the failed number of login attempts as a primary metric. Initial analysis indicated that KidsPic is a usable authentication for children. Thus in Chapter 5, I further enhanced the usability and theoretical password space of the KidsPic authentication mechanism. In Chapter 6, I describe the further research

on the KidsPic authentication mechanism with respect to both security and usability perspectives by conducting participatory design sessions and usability studies. Chapter 7 concludes this dissertation work and contains a summary of findings and provides possible future directions for continuing research in graphical authentication mechanisms for children.

CHAPTER 2

RELATED LITERATURE

Children create weak usernames and passwords [9, 7, 6, 8] yet are more likely to seek security advice and learn from it than adults and teenagers [18]. To develop an authentication mechanism for children that is both secure and memorable, we need to understand children's authentication practices and preferences. In this section, the literature is grouped into two general categories based on how a human brain remembers passwords and how humans access those memories [19]. The two general categories are recall-based passwords and recognition-based passwords. Alphanumeric authentication mechanisms are a recall-based authentication mechanism, and graphical authentication mechanisms are generally recognition-based and recall-based authentication mechanisms [20].

2.1 Recall-based - Alphanumeric Passwords

The alphanumeric authentication mechanism is one of the most used mechanisms for online authentication [21]. There are a variety of alphanumeric authentication mechanisms used for authentication based on system requirements. As passwords act as a key to any authentication mechanism, creating a password has many rules in

place. An alphanumeric password may include a combination of numbers, letters, and symbols. Both adults and children experience memorability issues using this mechanism due to its compound security rules for creating passwords [22, 9, 8, 23, 7, 24]. In order to overcome their memorability issues, children choose strategies that weaken the effectiveness of the authentication mechanisms like re-using their credentials across different account profiles and using a tool to remember credentials (e.g., writing passwords on a paper).

Although children have a theoretical understanding about when and why to use usernames and passwords for online applications, younger children tend to create short usernames and passwords compared to older children [8]. To understand the children's authentication practices with respective to alphanumeric authentication mechanisms, Read *et al.* conducted a qualitative study [8]. The study procedure includes researchers asking participants to create a username and a password with no restrictions. The younger children (ages 6-8) created shorter usernames and passwords when compared to older children (ages 9-10). The findings from Read *et al.* [8] do not support the findings from [6], where both younger and older children created short usernames and passwords. In [6], the authors noted that children tended to create short usernames and passwords to avoid memorability issues.

Children create usernames and passwords that are closely related to them (like, their pet's name or their last name as a password) [7]. In a study conducted by Lamichhane *et al.*, children created usernames and passwords which are self-related to them due to their memorability issues [7] and this correlates with Read *et al.* [8] study where, researchers found that child participants have memorability issues

with usernames and passwords [8]. To overcome their memorability issues, children are often dependent on adults (parents and teachers) to create and administer their usernames and passwords [23]. Adults play an important role in creating and administering their (children's) credentials because of their memorability issues. On the other hand, adults are encouraging children to adopt weak authentication practices such us using a tool (for instance, a container) to store the created passwords instead of suggesting strong authentication practices [23].

With password restrictions in place for online applications, children create their passwords obeying those restrictions [25]. In an attempt to understand children's online password behaviors, with 20 children (ages between 11 and 13), where child participants have to interact with three researcher's developed websites and create usernames and passwords [25]. All three websites require three different passwords with different password restrictions. As a result, children created self-related credentials. However, all of them created passwords with a combination of numbers, symbols, and text because of the password restrictions. In addition, authors from both studies [25, 6], believe that children are adopting their credential practices from adults (parents and teachers).

2.2 Recognition-based - Graphical Passwords

Humans have a better capability to recognize and recall visual information when compared to textual information (like, words and sentences) [11, 12, 13, 14, 15]. There is not much research on recognition-based authentication mechanisms designed for children therefore, we include recognition-based authentication mechanism literature

designed and evaluated with adults. With all of the usability and security challenges of alphanumeric authentication systems (which is pure recall-based), researchers believe that authentication through images can improve usability and security. The different kinds of graphical mechanisms can be grouped into two categories: recognition-based and cued recall.

In a recognition-based authentication mechanism, users have to recognize the previously chosen image for login from the registration phase. Recognition-based authentication systems are considered to be the easiest graphical mechanism for human memory. Passfaces^{TM} is one of the recognition-based graphical authentication mechanisms in which, random human faces are used for authentication [26]. In the Passfaces^{TM} mechanism, human faces are displayed in a grid view per web page and, a user has to select a set of (usually five faces; one face per grid) as their passwords during the registration phase. Next, the user has to recognize the chosen images in the registration phase in the same order during the login phase to get authenticated.

According to Tullis *et al.*, the Passfaces^{TM} mechanism is one of the graphical recognition-based authentication mechanisms which increases usability when compared to alphanumeric passwords [12]. A study conducted by Tullis *et al.* with 13 adult participants evaluated the memorability of this graphical authentication mechanism [12]. The graphical password authentication mechanism used in this study is similar to the Passfaces^{TM} mechanism with a 4x4 grid of images. The images used in their study however related to the participants were personal images of participants. In this study, twelve participants out of thirteen were successfully able to login to their accounts after six years.

In a modified Passfaces mechanism proposed by Grinal Tuscano *et al.*, the user has to enter their password by selecting their images from a 3X3 grid and enter text associated with it [27]. However, there was no evaluation study conducted by researchers. This mechanism is similar to a different mechanism proposed by Dunphy *et al.* [28], where a similar modified Pass Faces mechanism that requires users to describe the selected image as part of their password. During the login phase, images are displayed to users in a 3X3 grid based on the three experimental conditions (*Random groups*, *Visual groups*, and *Verbal groups*). In *Random groups*, the system fills a grid with one target image and eight other distraction images which match the gender of the target image. For example, if the target image is male, then the eight distraction images will be male. In *Visual groups*, the system fills a grid with one target image and eight other distraction images which match the description of the target image. In *Verbal groups*, the system fills a grid with one target image and eight other distraction images that match the verbal description of the images. The number of successful logins with the random are more compared to visual, and verbal experimental groups. Findings from the collected data suggest that participants did not find "Pass Faces with the description" useful and though to remember text for pictures as overhead.

Adults found a recognition-based authentication mechanism usable for daily authentication purposes [29, 30]. A study with two sessions to understand the picture preferences among users revealed that users (adults ages 18 to 43) are good at remembering objects as images as their passwords better than human faces and house images [29]. This study involves two sessions, in session one, students (n = 60) are assigned randomly to three different image types (faces, objects, and houses) used

in the authentication mechanisms. These authentication mechanisms are plugged-in for different open source websites. Students have to enter their passwords to use open-source websites. The study results suggested that human faces may not be the right pictures for authentication because there were more failed login attempts from participants when they used human faces for authentication and the houses picture authentication mechanism has the most number of login attempts. In the first session, the theoretical password space for a password is 28 bits where there were more failed login attempts. In the second session, researchers decreased the theoretical password space to 20 bits, and the number of failed login attempts are decreased. Though decreasing the password space increased the usability, on the other hand it reduced the security aspect of the authentication mechanism. A better authentication mechanism should maintain the balance of both usability and theoretical password space [31, 32].

The images' presentation affects the user choices in selecting images for a graphical password [33]. In an image-based graphical authentication mechanism, images play a vital role; it is essential to understand how pictures' presentation affects the user's choice in the user interface. Thorpe *et al.* conducted a study [33] in which they investigated the presentation effect on the graphical passwords by a user (n=34, ages of 18 and 30) at a university campus where participants are not from the computer science major. The images are presented to the users in a distinct fashion, "drawing the curtain" from right-to-left (RTL) and left-to-right (LTR). When the graphical system implements RTL, the leftmost grid columns are covered entirely and eventually revealed from the rightmost to the leftmost and vice-versa. Researchers observed the influence of the presentation effect from the collected data; participants selected the first visible image to them during curtain drawing from RTL and LTR. From the

observations of this study, it is clear that the presentation of images in graphical passwords affects the user's selection of images.

Davis *et al.* conducted a study with university students (n = 154) to understand the user authentication preferences between the commercially existing PassFace™ [26] and the developed mechanism *Story password* [30]. Users have to select four images as a password from four 3X3 grids in their proposed story password. The images used in this mechanism are related to nine categories: *"animals, cars, women, food, children, men, objects, nature, and sports"*. The two password mechanisms were plugged-in to the course website, and students should authenticate before accessing the course website. Results from the story password showed that participants could not remember the order of the pictures they selected for their story password.

2.3 Recall-based - Graphical Passwords

Recall-based graphical authentication mechanisms require users to recall their passwords during their login phase. Though recall-based graphical authentication mechanisms increase theoretical password space compared to alphanumeric authentication mechanisms, at the same time, it poses some usability challenges for users [34, 35]. Draw A Secret (DAS) is a graphical-based recall-based authentication mechanism where users have to draw something simple for their password in a 5X5 two-dimensional grid [34]. Though DAS increases the theoretical password space compared to the alphanumeric authentication mechanism, on the other hand, users have to draw their drawn passwords precisely into the grids, which affects the usability of the DAS authentication mechanism. For any authentication mechanism, it is

essential to balance both usability and security.

Children cannot remember their graphical click points passwords (with five click points in order) after ten days as well as they can remember an alphanumeric password [10]. In the cued click points authentication mechanism, the user chooses an image first and then clicks on various points in that image. The number of click points required as a password is dependent on the system requirements. A study conducted by Cole *et al.* with 13 child participants (ages between 6 and 12) asked children to create a textual password and a graphical password [10]. This study's graphical password interface requires users to select a picture first and then five click points on an image in sequential order. Five consecutive click points on a single picture act as a password. Using alphanumeric authentication mechanisms, users also created a password with no length or combination restrictions in place. Researchers in this study compared the participant's login attempts between both alphanumeric and graphical passwords. Participants had fewer failed login attempts for alphanumeric authentication mechanisms (84% success rate) compared to graphical passwords (71% success rate).

2.4 Previous Comparisons - Recall vs. Recognition

Although recognition-based graphical authentication mechanisms increase the ability to remember created passwords there are security holes introduced by using recognition-based graphical authentication mechanisms [36, 37, 38, 10, 39, 28, 33, 27, 12, 40, 30]. From the literature, it is clear that existing authentication mechanisms both alphanumeric and graphical (recognition-based and, cued click points

authentication mechanisms) are not very helpful for children; in other words, the present authentication mechanisms in the field do not provide usability (in-terms of memorability) for children. There is a need to develop and evaluate a graphical picture-based authentication mechanism with children which is usable and secure for children.

A study attempted to compare alternative password mechanisms (graphical authentication mechanism) with traditional authentication mechanisms (an alphanumeric authentication mechanism) for children, and found that children have memorability issues with a graphical mechanism where the password consists of clicking on certain points in a specific order on a picture [10].

We know from the literature that humans are better at recalling visual information than textual information [11, 12, 13, 14, 15]. As to maintain the balance between security and usability, we designed and evaluated a graphical user authentication mechanism, which consists of kid-friendly pictures called "KidsPic". We increased our proposed authentication mechanism's theoretical password space more than many existing picture-based graphical authentication mechanisms. Our initial formative studies revealed that children enjoyed using our proposed mechanism and remember the password after a week (98% success rate) compared to the alphanumeric password (75% success rate). Using our proposed system, we encouraged children to make a story while choosing images as their password. Children mentioned that creating a story to remember their password helped them recall their password after a week.

Based on the literature mentioned above in this chapter, that provides the basis for understanding general adult as well as some children's authentication practices.

There is a need to develop an authentication mechanism for children, which helps them create strong passwords and memorable passwords. As such, we designed and developed a graphical user authentication mechanism for children. A detailed explanation of procedures utilized to understand, design, create, evaluate, and improve a graphical-based authentication mechanism for children is articulated in the following chapters.

CHAPTER 3

UNDERSTANDING CHILDREN'S AUTHENTICATION PRACTICES

From the in-depth literature review in Chapter 2 it is clear that there is a need to understand children authentication practices with respect to a full array of security dimensions listed in Table 3.1 in a single study for children ages 5-11. Since security is multi-faceted, we posit that this more holistic approach can lead to better security practices. The main goal of this research was to better understand how elementary school children (ages 5-11) create and use usernames and passwords with respect to the security dimensions listed in Table 3.1 by conducting semi-structured interviews. Since parents and teachers can have an influence with regards to how children access online systems, we also surveyed adults in these roles as to their: (1) own understanding and practices with regard to authentication, and (2) perceptions of how children understand and utilize authentication mechanisms.

3.1 Methods Used

To better understand children authentication practices and adults' involvement in children online access, we conducted semi-structured interviews with children (n=22;

Table 3.1: A brief description of evaluation dimensions regards to usability and security

Security Category	Dimension	Description
Composition	**Security strength**	Creating usernames and passwords that include complex combinations of numbers, characters, and special characters.
	Self-related	Refers to how they make usernames and passwords, if they are related to them (e.g. their nickname, favorite superhero, name of their pet).
Performance	**Memorability**	How hard or easy the usernames and passwords are for children to remember.
	Error rate	How many errors children make while entering their usernames and passwords.
	Time to enter	The amount of time taken to enter their usernames and passwords when they are logging into applications.
	Over the shoulder	How concerned children are with someone watching them enter their credentials when logging in to devices/applications.
Mechanisms	**Usage in schools**	Objective is to understand how many applications/games children use and how differently they use at school from home.
	Reuse	How many times kids reuse their usernames and passwords through different applications they login in to.
	Preference	Describes what are the login preferences for children.
	Administration	To understand the involvement of adults in creating credentials for students.

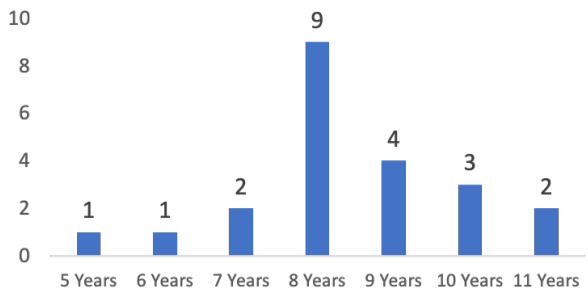


Figure 3.1: Age distribution of child participants

ages 5-11; see Figure 3.1 for the distribution of ages) and an online survey with adults (n=33; 25 parents, 5 teachers, 3 both parents and teacher). Approval was first garnered from the Institutional Review Board (IRB) and participants were recruited through localized social media and *Boys and Girls* clubs. Each participant (child and adult) received a $5 Amazon gift card for participating in this study.

Two researchers worked together to conduct each semi-structured interview: one to conduct the interview, and the other to take notes. The interviews lasted approximately 20-25 minutes each. Interviews were audio-recorded and later transcribed. The online survey took most adult participants 10-20 minutes to complete. The survey instrument (*Qualtrics*) recorded survey responses and later categorized and coded for analysis.

3.1.1 Interview Structure

The semi-structured interview conducted with children had four segments to it. Below are brief descriptions of each segment:

Table 3.2: Summary of some responses from child participants (age), children's stated preferred character length for username/password, entered alphanumeric username and passwords, the number of applications they use at home and school, number of applications they log into in a week. Grayed out cells are anonymized – a description of the original is given in brackets.

#	Age	Char Length uname/pword	Alphanumeric-Username	Length	Diff	Alphanumeric-Password	Length	Diff	# Apps	# Logins in a week
CP22	5		[child's name]	5	0	ariel	5	0	2	0
CP17	6		[child's school login]	9	-2	d1234	5	2	2	21
CP11	7	3	[child's initials]	1	2	123	3	0	1	3
CP8	7	10	[child's nickname]	6	4	[initials & birthday]	8	2	3	5
CP6	7	6	[child's name]	6	0	tmiewus	7	-1	0	0
CP1	8	Really short	nothing	7	—	password	8	—	2	Lot
CP2	8	4	2010	4	0	2810	4	0	1	0
CP3	8	7	[child's name]	14	-7	31589000	8	-1	3	2
CP9	8	4	[child's email]	31	-27	[initials & birthday]	8	-4	2	5
CP10	8	20	096457lhacer	12	8	1bnm	4	16	1	2
CP5	8	10	[child's nickname]	4	6	lava	4	6	3	2
CP12	8	5	Yogaboy	7	-2	[initials & birthday]	8	-3	4	4
CP15	8	12	lab11134	8	4	lab34	5	7	3	21
CP13	9	11	[child's name]	9	2	[initials & birthday]	8	3	4	12
CP14	9	3	[child's name]	3	0	4774	4	-1	4	2
CP16	9	4	supergirl[name]	14	-14	[brother]0314	12	-8	4	50
CP18	9	10	[child's school login]	9	1	fish20816@@	13	-3	4	3
CP4	10	4	serpentine	10	-6	2018??19	8	-4	0	0
CP20	10	9	[child's name]	9	0	[child's name & #]	14	-5	5	15
CP21	10	10	Derpy_Chicken2	14	-4	petsit123	9	1	6	1
CP7	11	10	[child's initials]	6	4	[garage code]	4	6	3	2
CP19	11	9	[child's school login]	9	0	88597	5	4	2	2

- **Segment 1:** We asked children to enter an alphanumeric username and password with no length or character combination restrictions. These were stored in a database and the usernames and passwords can be seen in Table 3.2.

- **Segment 2:** We asked child participants to create a pattern passcode using the basic Android-pattern mechanism (see Figure 3.2a, *left*). A screenshot was used to capture the password they entered.

- **Segment 3:** We then asked children 16 open-ended questions that related to the security dimensions above (see Table 3.3). Notes were taken on their responses and they were also recorded and transcribed.

- **Segment 4:** Children were asked to create a numeric password using the Android number passcode mechanism (see Figure 3.2b, *right*). A screenshot was used to capture the password they entered.

3.1.2 Adult Survey Structure

The online survey for adults consisted of two main parts after the consent form: (1) several questions related to the 10 authentication dimensions addressed above; and (2) the Security Behavior Intention scale (SeBIS) [1] questionnaire.

3.1.2.1 Questions Related to Authentication Dimensions

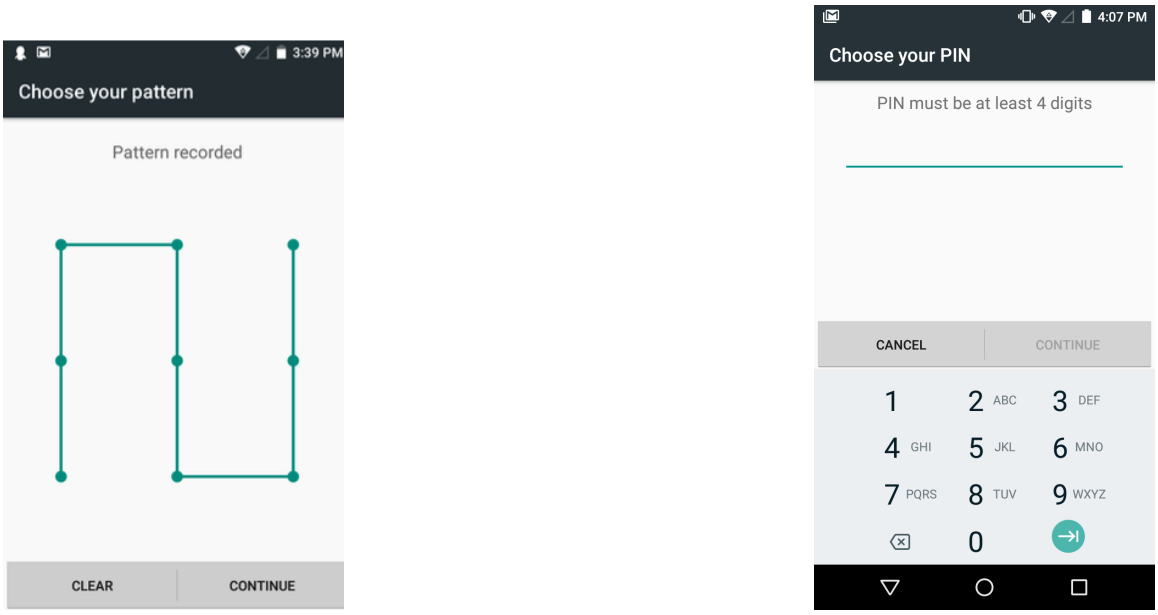
The questions in the first section was designed to understand adults' behavior in creating and using usernames and passwords, as well as their perceptions and

Table 3.3: Open-ended questions asked to child participants in Segment 3 of semi-structured interviews

Q#	Questions	Dimensions
Q1	What programs or apps do you use at home and at school?	Usage in schools
Q2	How many applications do you log into in a week?	Usage in schools
Q3	Do you have any shared devices(computers,tablets) at home?	Reuse
Q4	How many passwords do you have?	Security strength
Q5	What are the different ways you log into a computer?	Preference
Q6	Which mechanisms do you think is better and easier to use and why?	Preference
Q7	Do you use the same username and password for all the applications you login to?	Reuse
Q8	Who creates your usernames and passwords?	Administration
Q9	How often do you change your passwords?	Reuse
Q10	How do you remember your username and password?	Memorability
Q11	What do you think makes a good password in terms being a strong password?	Security strength
Q12	What do you think makes a good password in terms of being able to remember it?	Security strength
Q13	How many characters would you prefer to have for a username and password?	Security strength
Q14	Do you share your username and password with anyone close to you?	Over the shoulder
Q15	Do you use a tool for saving passwords? If so, what tool or app do you use?	Memorability
Q16	Has one of your accounts ever been locked due to entering your password wrong too many times?	Error rate

Table 3.4: Questions from *Qualtrics* survey for adult participants (excluding demographic and SeBIS questions).

	Q#	Questions
Comp.	1.	What do you think makes a good password?
	2.	What combination of characters makes a good password?
Performance	8.	As an adult, How good are you at remembering usernames and passwords?
	9.	What do you do to help you remember your usernames and passwords?
	10.	Please list all the tools you use to store your usernames and passwords.
	15.	How do you help your children to remember and save usernames and passwords?
	21.	How long does it take for your child to remember their username and password?
	22.	How long does it take for your child to enter their username and password?
	23.	How many times have you had to reset your computers/mobile devices due to multiple wrong entries of username and password by your child?
	24.	How many passwords do children need to remember? (please enter a number in the space provided below)
	25.	What strategies are you aware of that children use to remember their passwords?
	26.	How many mobile devices does your child use in your home? (including shared devices at home)
	31.	How concerned are children with someone else knowing their passwords? Please indicate the answer for each of the following groups of people:
	32.	How concerned are children with someone else being able to see them enter their password?
	39.	Have any of your children's accounts been hacked?
Mechanisms	3.	How often do you (as an adult) think you should change your password?
	4.	How often do you (as an adult) change your password?
	5.	Why don't you change it as frequently as you say you should?
	6.	How often do you think children should change their passwords?
	7.	How often do you think children actually change their passwords?
	11.	Do you as a parent play a role in creating your children's passwords?
	12.	Do you as a teacher play a role in creating your children's passwords?
	13.	Do you as an IT admin play a role in creating your children's passwords?
	14.	What role do you play in creating children's passwords?
	16.	How easy for you to create usernames and passwords for your children?
	17.	What is easy about creating usernames and passwords for your children?
	18.	What is hard about creating usernames and passwords for your children?
	19.	What devices do you enter a password on? (You can select one or more options)
	20.	How do passwords differ on each device? (If applicable, please select one or more options for a single device)
	27.	Do multiple devices at your home share the same password(s)?
	28.	How often do your children reuse their username and password across multiple applications/devices?
	29.	How safe do you (as an adult) think it is to use the same username across the multiple applications?
	30.	How often do you (as an adult) use the same username for applications you use (so it is easy to remember)?
	33.	Who decides what the username and password are for children's accounts?
	34.	For previous question you selected: . For each group, please explain how they decide what the username and password are?
	35.	Do teachers talk to children about how to create usernames and passwords?
	36.	What instructions do teachers give to children about creating usernames and passwords?
	37.	What instructions do you as a teacher give to children about creating usernames and passwords?
	38.	What instructions do teachers give to children about security?



(a) **(b)**

Figure 3.2: (a) Android's pattern passcode interface used in the study. (b) Android's numeric passcode interface used in the study.

involvement in authentication practices for children. It consisted of several questions and the survey was administered as a *"Qualtrics"* survey (See Table 3.4).

3.1.2.2 SeBIS Scale and Structure

The second section of the *adult* survey consisted of questions to evaluate the general security behaviors of adults. To do this, we utilized the Security Behavior Intentions Scale (SeBIS) [1]. The SeBIS scale asks questions in four categories: device securement (locking computers and mobile devices, and using password or passcode), password generation (creating and using passwords for devices), proactive awareness (being aware of potential risks and exercising precaution), and updating (upgrading software and using anti-virus). Participants were asked to respond to the questions

from Table 3.5 on a 1-5 scale: (1) Never, (2) Rarely, (3) Sometimes, (4) Often, and (5) Always. The scale is sometimes inverted for improved validity, during its administration, but for presentation here, all answers are aligned to facilitate the interpretation of results. The presentation order of the questions is also randomized. For each question in the four sections the mean (μ), standard deviation (σ), and median were calculated for both the parents (15 adults) and teachers (4 adults) (see Table 3.5). As the sample size is small, we compared the medians (or the location on the scale) of the two group's responses.

3.1.2.3 Demographics of Adult participants

Of the 33 adult participants (ages 26-58; μ=40.3, σ=7.87), 55% have an undergraduate degree, 15% have a graduate degree, 15% have a high school degree, 3% have an associate degree, and 6% have no degree. The median income of our participants is ($75,000-$99,000), with a minimum of (<$20,000), and maximum of (>$100,000). Out of the 33 adult participants, 19 participants answered every question on the SeBIS scale. We removed all participants' responses who did not answer all of the questions in this section. One participant's data was removed from analysis, as it was incomplete due to audio-recording issues.

3.2 Findings & Analysis

As noted above, all semi-structured interviews were audio recorded and transcriptions were made and stored using *NVivo* (version 12) for qualitative analysis. The questions asked in the interviews are listed in the Table 3.3.

Table 3.5: Parent and teacher responses using the SeBIS scale [1]. SeBIS utilizes a five point scale from: (1) Never, (2) Rarely, (3) Sometimes, (4) Often and, (5) Always). The overall (parents and teachers) mean (μ), standard deviation (σ), the mean (μ), standard deviation (σ), and median are displayed for both parents and teachers group.

	#	Questions	Overall		Parent's Response			Teacher's Response		
			μ	σ	μ	σ	**median**	μ	σ	**median**
Device Securement	F3	I manually lock my computer screen when I step away from it.	3.10	1.44	3.30	1.30	3.5	3.00	2.00	2.0
	F4	I set my computer screen to automatically lock if I don't use it for a prolonged period of time.	3.89	1.33	4.06	1.12	4.0	3.25	1.78	3.5
	F5	I use a PIN or passcode to unlock my mobile phone.	3.52	1.66	3.93	1.38	5.0	2.00	1.73	1.0
	F6	I use a password/passcode to unlock my laptop or tablet.	3.94	1.43	4.2	1.10	5.0	3.00	2.00	3.0
Password Generation.	F12	I do not change my passwords unless I have to.	2.31	0.86	2.4	0.95	2.0	2.00	0.00	2.0
	F13	I use different passwords for different accounts that I have.	3.36	1.17	3.46	1.14	4.0	3.00	1.22	2.5
	F14	I do not include special characters in my password if it's not required.	2.68	1.29	2.73	1.33	2.0	2.5	1.1	2.5
	F15	When I create a new online account, I try to use a pwd that goes beyond the site's min requirements.	3.31	1.07	3.33	1.07	3.0	3.25	1.08	3.0
Proactive Awareness	F7	If I discover a security problem, it continue what I was doing because I assume someone else will fix it.	2.10	0.85	2.13	0.88	2.0	2.00	0.70	2.0
	F8	When someone sends me a link. I open it without first verifying where it goes.	2.31	0.86	2.57	0.90	3.0	3.00	1.00	3.0
	F10	When browsing websites, I mouse over links to see where they go, before clicking them.	3.00	0.85	3.06	0.85	3.0	2.75	0.82	2.5
	F11	I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar.	2.57	0.99	2.26	0.92	2.0	2.00	0.70	2.0
	F16	I submit info to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon).	2.21	0.89	1.93	0.77	2.0	2.00	0.00	2.0
Updating	F1	When I'm prompted about a software update, I install it right away.	3.10	1.16	3.2	1.22	3.0	2.75	0.82	2.5
	F2	I try to make sure that the programs I use are up-to-date.	3.10	1.16	3.66	1.01	4.0	3.75	1.08	4.0
	F9	I verify that my anti-virus software has been regularly updating itself.	3.52	1.22	3.4	1.20	4.0	4.00	1.22	4.5

For ease of referencing we will refer to child participants as CPX where X is a number. The analysis was conducted using an inductive approach to develop codes and categories by the authors reviewing the responses to the semi-structured interviews (transcribed from children responses) and surveys (as typed by the adults) [41, 42]. In the remainder of this section we discuss the responses in relation to the dimensions in Table 3.1 (Composition, Performance and Mechanisms) and the codes, categories were created through the analysis. We compare and contrast the responses between adults and children where appropriate. Participant counts are identified in parenthesis in the analysis and discussion below.

3.2.1 Composition

3.2.1.1 Security Strength

For evaluating the credentials composition dimension, we asked adults an open-ended question, "What do you think makes a good password?" 58% of participants (19 of 33) explicitly mentioned that good passwords include combinations of characters, numbers, and special characters. However, when adults were asked directly "What combination of characters makes a good password?", 100% of our participants (33 of 33) indicated the importance of combinations of elements (e.g. letters, numbers, and/or special characters) in their passwords. 9% of participants (3 of 33) mentioned the need for random passwords. When children were asked, "What do you think makes a good password in terms of being a strong password?", 54% of child participants (12 of 22) mentioned the need to include combinations of numbers, letters, and/or special characters; 14% (3 of 22) mentioned the need to randomly arrange characters when

creating a good password.

One of the questions to children was, "How many characters would you prefer to have for a username and password?" The responses were analyzed using the categories from [8] (length in characters, 0-5, >5-10, >10-15, >15-20). We used their categories in order to compare our results with their data. They recruited 49 children for the second part of the study in which they had analyzed the lengths of usernames and passwords created by children, (ages 6-7(n=26), and 9-10(n=23)), their results for younger children (usernames: μ=7.08, σ=4.19; passwords: μ=5.88, σ=3.01) when compared to the older children (usernames: μ=10.91, σ=4.04; passwords: μ=7.52, σ=2.81). Child participants in our study chose the same number of characters in length for both username and password. The results from our children (ages 5-11) interviews therefore had the same means and standard deviation for both usernames and passwords (μ=7.76, σ=3.95). The mean from our results is similar to that of the older children passwords in [8], however ours had a larger standard deviation. The preferred length of the usernames and passwords chosen by our *child* participants are shown in Figure 3.3.

In our semi-structured interviews we not only had their stated preferences, but also collected observational data as we asked children to create an alphanumeric username and password (with no restrictions) so we could observe the patterns and composition of their usernames and passwords. Table 3.6 shows the usernames and passwords they created along with their associated character lengths. In many cases the username or password is *anonymized* so as to not reveal information about the participants. The data shows there is a difference between their stated preference and the actual

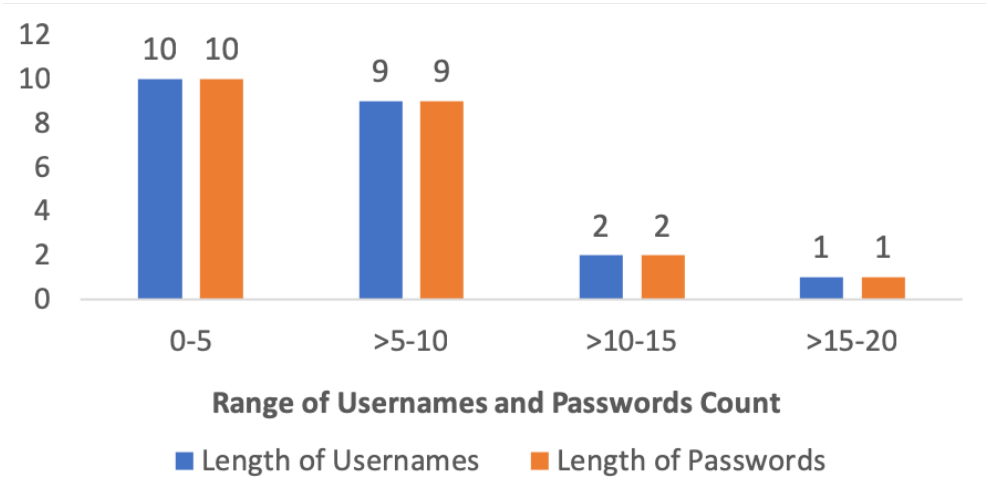


Figure 3.3: Username and Password length preference by children. We can observe that children created usernames and passwords are same size.

creation of username and password with regards to length (see the 'Diff' in Table 3.6). Three children (ages 5, 6, and 7) struggled to come up with a username and password as they did not know how to spell their desired usernames and passwords. For example CP6 said that she wants to enter her password as *"time is waste"* and she entered *"tmiewus"*. The other children displayed the ability to create usernames and passwords with combinations of letters.

3.2.1.2 Self-Related

In addition to the length and complexity of the usernames and passwords, as can be seen from Table 3.6, there were several that related to the participants fitting within the composition dimension of *self-related*. Some of them related directly to themselves using their name or initials, in fact, 68% (15 of 22) used their name or something otherwise very identifiable for their username (which is not too surprising).

Table 3.6: Summary of some responses from child participants (age), children's stated preferred character length for username/password, entered alphanumeric username and passwords, the number of applications they use at home and school, number of applications they log into in a week. Grayed out cells are anonymized – a description of the original is given in brackets.

#	Age	Alphanumeric-Username	Length	Char Length uname/pword	Diff	Alphanumeric-Password	Length	Diff	# Apps	# Logins in a week
CP22	5	5	[child's name]	5	0	ariel	5	0	2	0
CP17	6	7	[child's school login]	9	-2	d1234	5	2	2	21
CP11	7	3	[child's initials]	1	2	123	3	0	1	3
CP8	7	10	[child's nickname]	6	4	[initials & birthday]	8	2	3	5
CP6	7	6	[child's name]	6	0	tmiewus	7	-1	0	0
CP1	8	Really short	nothing	7	—	password	8	—	2	Lot
CP2	8	4	2010	4	0	2810	4	0	1	0
CP3	8	7	[child's name]	14	-7	31589000	8	-1	3	2
CP9	8	4	[child's email]	31	-27	[initials & birthday]	8	-4	2	5
CP10	8	20	0964571hacer	12	8	1bnm	4	16	1	2
CP5	8	10	[child's nickname]	4	6	lava	4	6	3	2
CP12	8	5	Yogaboy	7	-2	[initials & birthday]	8	-3	4	4
CP15	8	12	lab11134	8	4	lab34	5	7	3	21
CP13	9	11	[child's name]	9	2	[initials & birthday]	8	3	4	12
CP14	9	3	[child's name]	3	0	4774	4	-1	4	2
CP16	9	4	supergirl[name]	14	-10	[brother]0314	12	-8	4	50
CP18	9	10	[child's school login]	9	1	fish20816@@	13	-3	4	3
CP4	10	4	serpentine	10	-6	2018??19	8	-4	0	0
CP20	10	9	[child's name]	9	0	[child's name & #]	14	-5	5	15
CP21	10	10	Derpy_Chicken2	14	-4	petsit123	9	1	6	1
CP7	11	10	[child's initials]	6	4	[garage code]	4	6	3	2
CP19	11	9	[child's school login]	9	0	88597	5	4	2	2

32% (7 of 22) used something self-related in their password. CP7 for example created his password and mentioned to researchers the password he used was his "garage code". This re-use also applies later to our discussion of memorability and re-use.

Similarly, CP19 created both her username and password which are in no way related to her name or her personal information. She mentioned that her school and family encourage her to create usernames and passwords for online applications which should not include any personal information. Another participant, CP4, used her pet name as a username and mentioned that she can easily remember her username and password which includes a combination of special characters and randomness. This displays an understanding of how to create a strong password using combinations and also how creating a username that is self-related can improve memorability.

3.2.2 Performance

3.2.2.1 Memorability

Several questions related to memorability were asked, such as a question to child participants "How do you remember your usernames and passwords?" 55% (12 of 22) of child participants answered, they would practice by entering multiple times. To know the adult's perception, we asked the same question in the survey as "What strategies are you aware of that children use to remember their passwords?" 30% (10 of 33) of adult participants responded that children always use self-related things to create usernames and passwords. From Table 3.6 we can see that most of the children in this study created their credentials by using information that was related to themselves (self-related) and adult participants said that children would write

them down (18%; 6 of 33) and repeat them multiple times (21%; 7 of 33). Another question to child participants was “Do you use any tool to save your usernames and passwords?”. 54% (12 of 22) of child participants indicated they use a tool for saving their credentials. Of those, half of them (6 of 12) use a tool (e.g, save them in browser, icloud), and the other half (6 of 12) use a piece of paper to remember their credentials. 45% (15 of 33) adult participants replied that they *(adults)* use a piece of a paper as a tool for saving their credentials, this corroborates with the children’s response "write them on a paper". We asked child participants, “What do you think makes a good password in terms of being able to remember it?” 59% (13 of 22) of child participants said they would choose credentials which are related to their likes (e.g, favourite super hero, pet name) or otherwise related to themselves (e.g, their name, siblings name) so they could better remember them. Responses suggest that children in this study have an understanding that they have to create usernames and passwords that involve randomness, on the other hand they have memorability issues, so many of them end up creating credentials which are *self-related*.

3.2.2.2 Error Rate

An error rate security dimension question to children was “Has one of your accounts ever been locked due to entering your password wrong too many times?” 45% (10 of 22) of child participants said their accounts got locked. A similar question was asked of adults, and 67% (22 of 33) replied that their devices had been locked at least one to two times due to children entering their credentials wrong multiple times.

3.2.2.3 Time Taken to Enter

We asked adults "How long does it take for your child to enter their username and passwords?" which focuses on the time taken to enter username and passwords. 36% (12 of 33) of adult participants answered their children would take "11-20 seconds" to enter their credentials however, from the researchers observation in semi-structured interview sessions children took more than "11-20" seconds to enter their credentials.

3.2.2.4 Over the Shoulder and Sharing

When children were asked to create an alphanumeric, pattern, and numeric passwords they readily did so in the researcher's presence and were not at all bothered about researchers watching them create and enter their credentials. This could be due to the fact that the children trusted the researchers or were making an exception, or it could be that children are less aware of how others can learn a password by watching them. Interestingly, when we asked adults "How concerned are your children entering their credentials in the presence of someone?" 61% (20 of 33) of adult participants said their children are concerned. 68% (22 of 33) of child participants said they would share their usernames and passwords with someone close to them. 64% (14 of 22) of child participants indicated they would share their credentials with their *parents*, 50% (11 of 22) with their siblings, 36% (8 of 22) would share them with their *teachers*, and only 14% (3 of 22) with their peers. In summary, adults note that children are concerned with someone watching or knowing their credentials and children share this concern but are willing to share them with certain groups of people most of which are parents and least of which are peers.

Three of the teacher participants in our study said that a couple of their student accounts were "hacked" describing it as one student's credentials were entered by another student which is illustrative of what teachers view hacking of a children's account to be.

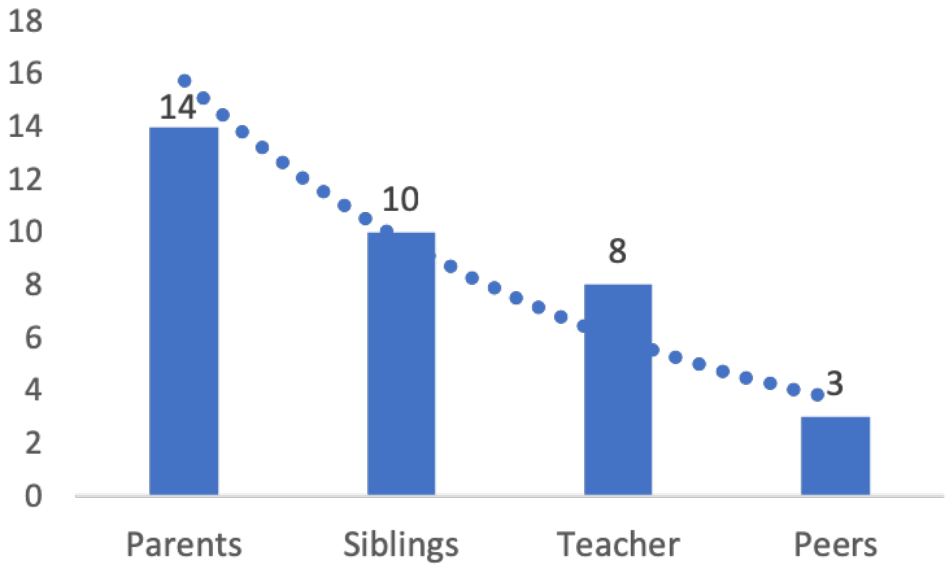


Figure 3.4: Child participant's opinion on sharing credentials.

3.2.3 Mechanisms

3.2.3.1 Usage in Schools

As part of usage in schools, we asked children "what are the different applications you use at school?" 77% (17 of 22) of participants responded that they use at least one. For the question which we asked in the survey for adults "Do teachers talk to children about how to create usernames and passwords?" 36% (12 of 33) of participants said teachers do talk to children about how to create usernames and passwords. Another

question for adults was "What instructions do teachers give to children about *creating usernames and passwords*?" A teacher replied that she suggests to children not to create credentials which includes personal information, and 27% (9 of 33) said they are not aware of the instructions given by teachers to children about creating username and passwords. From the adult perspective, when we asked "What instructions do teachers give to children about *security*?," 33% (11 of 33) of participants said they were unsure of the instructions given by teachers to students, 9% (3 of 33) of the adult participants replied that teachers suggest children not to share their credentials. From the responses to these questions, we can say that children seem to not be getting adequate education about authentication and security from their parents or teachers.

3.2.3.2 Re-use

A majority of the child participants 86% (19 of 22), said they have 1-3 passwords, and 76% of adult participants said children would have 1-3 passwords. Figure 3.5 depicts how there is a slight skew towards adults thinking children have more passwords than children think they have. When children were asked "Do you use the same username and password for all the applications you login to?" 63% (14 of 22) said that they would not reuse them for different applications. 42% (14 of 33) of adults responded to this question as children sometimes reuse their credentials and 27% (9 of 33) of participants responded that children always reuse their credentials. We asked a question to adults, "How safe do you think it is to use the same username and password across the multiple applications?", 52% (17 of 33) said it is not safe, and 39% (13 of 33) said they have no idea about it. The follow-up question to adults was "How often do you (as an adult) use the same username for applications you use

(so it is easy to remember)?" 45% (15 of 33) of adult participants said they reuse their credentials most of the time, and 27% (9 of 33) of adults replied they always reuse their credentials. These responses from adults illustrate that children and adults frequently reuse their credentials due to memorability issues.

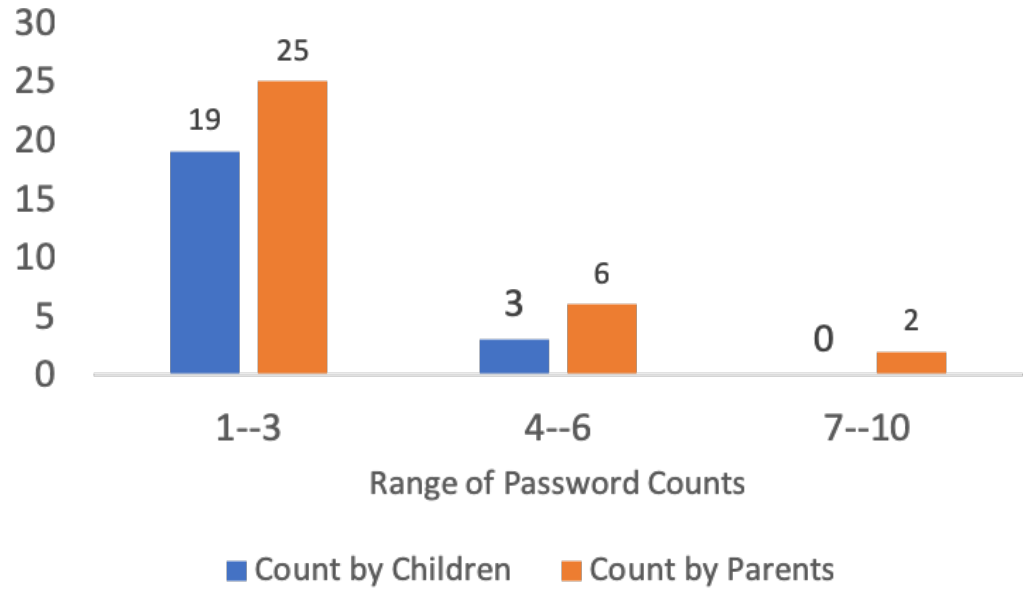


Figure 3.5: Number of passwords children have and the adults perception about the passwords that children would have.

In addition, when child participants were asked how often they changed their credentials 77% (17 of 22) indicated they would not change their credentials, and 54% (18 of 33) of adult participants said that, children would never change their credentials. We also asked adult participants about their own understanding and practices, in theory they understood the need to change the credentials, but in practice they did not do it as frequently as they said they should in theory. Figure 3.6 shows the difference between the adult's theoretical understanding versus their actual practice in changing their authentication credentials. The trend lines show how they understand

that they should change their passwords frequently, but they do not do it as frequently as they know they should.

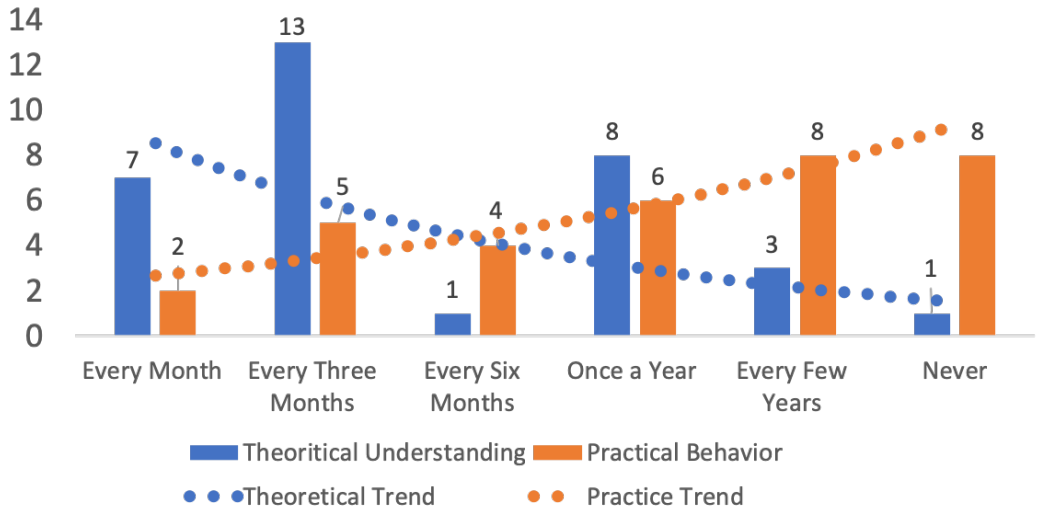


Figure 3.6: Adult's theoretical understanding versus their actual practices of changing their passwords.

3.2.3.3 Preference

82% (18 of 22) of child participants said they would prefer alphanumeric password mechanisms over pattern and number password mechanisms. Two participants said they never had an interaction with pattern mechanisms and two said they would prefer this pattern as it is very fast and easy to remember in their perception.

With regards to the number of devices used by children, 77% (17 of 22) of child participants indicate they have at least one shared device at home. In a similar vein, 87% (29 of 33) of adult participants responded saying they share their devices with their children. Each child's reported number of applications and logins in a week is

presented in the last two columns of Table 3.6.

3.2.3.4 Administration

In terms of general administrative practices related to authentication, we asked adults "Do you as a teacher or parent play any role in creating your children's passwords?" 77% (25 of 33) of adult participants replied that they played a role in creating them and 68% (17 of 25) of the adult participants replied that either they create credentials for their children or they worked with their children to create them. This reveals that adults play an important role in creating credentials for their children. We also asked adults "How do you help your children to remember and save usernames and passwords?" 33% (10 of 33) of participants said they will write them down for their children and 63% (21 of 33) of participants said that they would help children make credentials that are self-related to children, so they (*children*) can easily remember them. This differs from another study that was conducted via semi-structured interviews with children and parents (aged 7-11) where parents reported they *always* had a copy of their child's account information [43].

3.2.4 Parent and Teacher SeBIS Responses

In this section we analyze and discuss data from the 19 adult participants who responded to all of the questions on the SeBIS scale (see Table 3.5 for all of the SeBIS questions). We analyze their responses in terms of parent (n=15) and teacher (n=4) responses to better understand their security practices. There are four sections in SeBIS: device securement, password generation, proactive awareness, and updating.

All of these areas fall within the dimension of *administration* except the questions in the password generation section. The four questions in the password generation section relate to various other of the authentication dimensions: F12 *(administration)*, F13 *(Reuse)*, and F14 & F15 *(security strength)*. The scale for each question is: (1) Never, (2) Rarely, (3) Sometimes, (4) Often, and (5) Always. The mean (μ), standard deviation (σ), and median for each sections can be found in Table 3.5.

3.2.4.1 Device Securement

The device securement SeBIS questions (F3, F4, F5, F6 in Table 3.5) all relate to the administration dimension.

For question **F4**, the median response for the parents group was 4.0 which suggests *often* parents set their screens to automatically lock when it is not in use for a long period of time. The median for the teachers was 3.5 which suggests that most responses fall in between *sometime* and *often*. For question **F6**, the median response for the parents group was 5.0 which implies parents *always* manually lock their computer screen when they step away from it. While this is a good security practice, it was surprising that most parent's adhere to this. On the other hand, the median responses from teachers was 3.0 indicating they *sometimes* manually lock their computer screen when they step away from it. For question **F3**, the median response for the parents group was 3.5 so most responses fall between *sometimes* and *often*, and for teachers it was 2.0 indicating they *rarely* manually lock their computer screen when they step away from it. For the question **F5**, the median response for the parents group was 5.0 which indicates parent participants *always* use a passcode

to unlock their mobile phones; where teachers in our sample had a median of 1.0 suggesting they *never* use a passcode to unlock their mobile phones.

Median responses for the above questions, suggest differences between teachers and parents in terms of device securement, and that for our sample, parents followed better security practices more frequently than the teachers.

3.2.4.2 Password Generation

For the question **F12**, median responses from parent and teacher groups was 2.0 indicating they *rarely* do not change their password unless they have to. For the question **F13**, median response for the parents group was 4.0 indicating they *often* use different password for different accounts, whereas teachers' median response was 2.5 indicating between *rarely* and *sometimes* that they use a different password. This suggests again, that in our sample, parent's practices are more aligned with better security practices as compared to teachers.

In contrast, for the question **F14**, the median response for the parents group was 2.0 suggesting they *rarely* include special characters in their passwords if it is not required, the median response for teachers was only slightly higher at 2.5. For the question **F15**, median response for the parent and teacher group was 3.0 for both suggesting they only *sometimes* use a password that goes beyond my site requirements. There no significant difference between teacher and parent groups for the questions **F14** and **F15** that relate to security strength.

3.2.4.3 Proactive Awareness

In this section, all the questions are related to the administration dimension. For question **F7**, the median response for the parents and teachers was 2.0 which indicate they *rarely* bother with security problems they encounter and assume someone else will fix it. Question **F8**, also has the same median response for parents and teachers at 3.0 indicating they *sometimes* will visit a link sent to them without first verifying where it goes. Similarly for question **F10**, median responses for parents (3.0) and teachers (2.5) indicate they *sometimes* open a link while browsing website without checking the link first. Both parents and teachers have the same median response of 2.0 for question **F11** indicating they *rarely* know the website based on its look and feel. For the question **F16**, median response for the parents and teachers was 2.0 – that they *rarely* submit the information to websites without verifying it will be sent securely (e.g. SSL, HTTPS). *Teachers* median response was also 2.0 *rarely*. Both parents and adults are similar on all questions in this area. While responses to the last question are more encouraging than the others, as a whole with regards to proactive awareness both parents and teachers responses indicate some vulnerabilities for both groups in this area, suggesting areas for improvement.

3.2.4.4 Updating

All the questions asked in this section also relate to the administration security dimension and all are generally similar for both parents and adults. Question **F1**'s median response for parents was 3.0 and 2.5 for teachers which indicates they *sometimes* update software when prompted to do so. For the question **F2**, median responses for

the parents and teachers was 4.0 indicating they *often* make sure the programs they use are up to date. For the question **F9**, the median response for the parent group was 4.0 and teachers 4.5 indicating they *often* to *always* make sure their anti-virus is regularly updating by itself.

3.3 Discussion

In this chapter we presented the results from interviews of children and a survey of adults that elucidates children's understanding and practices with regards to authentication. Most of the children and adults in this study have a theoretical knowledge about credentials creation and usage but do not implement that knowledge in their practices. There is a large discrepancy in the number of characters they would want in their credentials and the number of characters children actually included when they are asked to create one, this impacts the *security strength* of their authentication.

The younger children in our study faced some issues with spelling their usernames and passwords, and most of the children created credentials that are *self-related* or even duplicated from other logins that they have. Children tend to create usernames and passwords that are self-related and write them down on a paper or use a tool to increase the *memorability* of their authentication credentials. Due to *memorability* issues many parents reported that their children had locked their applications or devices by entering wrong username and passwords which indicates a large *error rate* in the login mechanisms. According to researchers' observations, children's *time taken to enter* their credentials was more than 20 seconds.

In our study, no child participant was concerned that researchers were watching them enter their usernames and passwords. And most children were willing to share their passwords with a parent, but less so with a sibling or teacher, and even less so with a peer. Every child participant needed to use authentication credentials with at least one application either at school or at home. Surprisingly, the majority of the child participants said they would not *reuse* their credentials for different applications, however, our observations illustrated that this was not necessarily the case as children created new logins (re)using credentials they previously had on other systems. All child participants had experience with a computer and keyboard, and all preferred the alphanumeric mechanism for logging in (as opposed to number and pattern). Most adults in our study indicated that they play a role in creating and using credentials for their children. In addition, observations from our sample indicate that both children and teachers can improve their authentication practices, indicating the need for further education for teachers and children regarding secure authentication practices.

SeBIS responses from adults suggest that there is a gap in adult's knowledge in terms of security behaviors. There are noticeable differences in the theoretical and actual behaviors with adults as they create and re-use credentials. We observed from the collected results and analysis that both adults and children use weak authentication practices. There is a need to improve their authentication practices, one way to do so is to develop an authentication mechanism that avoids memorability issues and provides a reasonable level of security.

CHAPTER 4

GRAPHICAL USER AUTHENTICATION MECHANISM (KidsPic) FOR CHILDREN

From the study presented in *Chapter 3*, we observed that all the child participants used technology that requires them to make a username and password. While children mentioned that they do not reuse their usernames and passwords, most of them reused their credentials when we asked them to create a username and password. Reusing credentials indicates that they have memorability issues with using usernames and passwords. Adults (parents and teachers) often help children with usernames and passwords because of their memorability issues. From *Chapter 2* and the results and analysis of collected data from *Chapter 3*, it is clear that there is a need to develop an authentication mechanism for children that would reduce memorability issues.

To develop an authentication mechanism for children that can reduce their memorability issues and provide online security, it is essential to understand further children's authentication preferences. We considered alphanumeric and graphical picture-based authentication mechanism to understand their authentication preferences. This chapter will explain the four different formative studies we conducted in series to understand children's authentication preferences. We asked children (n

= 8; μ age = 8.3) to create a username and password and to later login with those usernames and passwords using three different authentication mechanisms.

4.1 Methods Used

To understand children's authentication practices and their preferences with authentication mechanisms, we developed and utilized two authentication mechanisms. The two authentication mechanisms are an *alphanumeric authentication mechanism* and a $KidsPic_{16|4}$ a novel graphical-based authentication mechanism.

- **Alphanumeric Authentication (without password length restrictions):** In this mechanism, no restrictions were specified and children were able to use as many characters and their choice of character combinations to create a username and password.

- **Alphanumeric Authentication (with password length restrictions):** In this mechanism, length restrictions were specified. Children had to create a password, with at least eight characters. Please see Figure 4.1 for the user interface for the alphanumeric mechanism with length restriction in place.

- **KidsPic Authentication:** KidsPic is a graphical authentication mechanism in which a username is alphanumeric and the password is selected from a set of unique pictures. In this study the KidsPic authentication mechanism, used four sets of images, and each set contained 16 unique pictures (in a 4X4 grid). Since we discuss variations of KidsPic later in this chapter, we identify this version

Figure 4.1: Screenshot of a developed alphanumeric authentication mechanism with password length restriction in place.

by the number of pictures in each set (16) and the number of sets (4), in this manner: KidsPic$_{16|4}$ (see Figure 4.2).

4.2 Research Questions for the Formative Studies

Below are the research questions which helped us to understand children's authentication practices between alphanumeric and KidsPic$_{16|4}$ authentication mechanisms – the primary research question posed in the introduction (Chapter 1). The findings from the research questions helped us to observe that KidsPic$_{16|4}$ helped children remember their created passwords in both short- (15 minute) and long-term (1 week) situations.

- **RQ1:** Can children remember a newly created username and password (with no password length restrictions) after fifteen minutes of distraction activity and after a week?

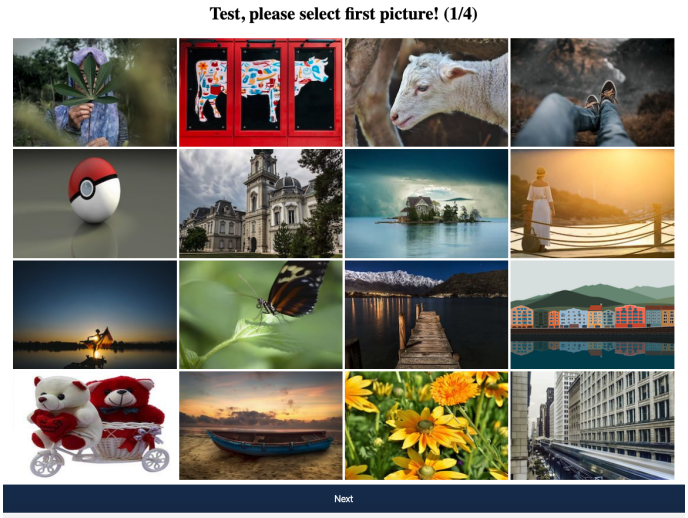


Figure 4.2: Screenshot of KidsPic$_{16|4}$ authentication mechanism displaying pictures sixteen pictures in total.

- **RQ2:** Can children remember a newly created username and password (with password length restrictions) after fifteen minutes of distraction activity and after a week?

- **RQ3:** Can children remember a KidsPic$_{16|4}$ password better than an alphanumeric password?

- **RQ4:** How will an educational video on "how and why to create a strong username and password" influence children to create a strong username and password?

  - **RQ4(a):** Do children create a strong username and password after watching a password educational video?

  - **RQ4(b):** Can children remember a newly created username and password after a password educational video and fifteen minutes of a distraction

activity and after a week?

We conducted a series of formative studies to address the research questions, where children created different usernames and passwords using alphanumeric and the KidsPic$_{16|4}$. Below are brief descriptions of each session.

- **Session One:** In session one, children created a username and password using a standard alphanumeric authentication mechanism (with no password length restriction). After creating a username and password, children played an online game from PBS KIDS [1] for fifteen minutes and returned to the system to enter their created username and password.

- **Session Two:** This session took place after a week from the first session. In this session, at first, children entered their usernames and passwords, which they created in the first session. Secondly, children created two different usernames and passwords, one using Alphanumeric authentication mechanism and second using the KidsPic$_{16|4}$ authentication mechanism. At last, children played a child-appropriate online game from PBS KIDS for fifteen minutes and entered their created usernames and passwords from this session.

- **Session Three:** This session occurred one week after the second session. In this session, children first entered their usernames and passwords from the second session. Next, children watched an educational video that explains "How and why to create a strong username and password using alphanumeric authentication mechanism[2]." After watching the video, children created a

[1] `https://pbskids.org/`
[2] `http://bit.ly/StrongPasswordVideo`

username and password using the alphanumeric authentication mechanism. After creating a new set of username and password, children played a video game from PBS KIDS for fifteen minutes. Finally, children returned to the system after fifteen minutes to enter their created username and password.

- **Session Four:** Session four took place a week after the third session. In this session, children entered their username and password from the third session.

4.3 Findings & Discussion From the Formative Studies

In the first session, children created username and password with no password length restrictions, see in Table 4.1. Statistical significance for failed number of login attempts and time taken to enter the password was determined based on a paired t-test ($p<0.05$) using GraphPad Prism 8.01 software[3]. Unless otherwise noted, data represent mean Standard Error of Means (± SEM). All the participants, except one (age = 11, number of attempts = 11), entered correct usernames and passwords in a single attempt after fifteen minutes of a distraction task. Interestingly, in the second session after a week, the number of failed login attempts increased ($\mu = 8.5$) with a p value of 0.07, in comparison to the first session. See Figure 4.3a.

In the second session, during the registration phase, children created usernames and passwords for two different authentication mechanisms. See in Table 4.1 for created alphanumeric usernames and passwords by children with password length restrictions. The number of failed login attempts for alphanumeric mechanism ($n =$

[3] `https://www.graphpad.com/`

Table 4.1: Summary of alphanumeric usernames and passwords created by children in formative studies with their respective age. In the table, fn represents, first name; ln represents, last name; fl represents full name.

		With out Password Length Restrictions		**With Password Length Restrictions**		**After Watching a Video**	
#	Age	Username	Password	Username	Password	Username	Password
P1	6	fgd	cat	sda	dogcatdo	cvb	cdoacdoa
P2	6	2erv	child fn	mklio	[child fl]	[child fn]	[child fl dot]
P3	7	child fn	4444	child fn	[child fn]444	@@@@[child fl]	@@@@[child fl]
P4	8	[child initials]1	1235	[child initials]1	12345678	[child initials]123	97531
P5	9	[child fn initial][child ln]	LOVE [Univ acronym]	ilovepuppys	puppycute	#PuppyLove	#PuppysRock
P6	9	KittyMeowMeow	KittypufferFosh321	MeowKittyMeow	Kittypufferfosh234	Meowwwwwwwww	IlCrN@net
P7	11	Boris the woof	FAVORITE BONE123	Gbo	pooppoop	gbo	tloz0911#
P8	11	PI-thon	3.14-noodleboop	BoopableMath	CatthonofSmarts	CrazyKitty3.14	wIUs2009?

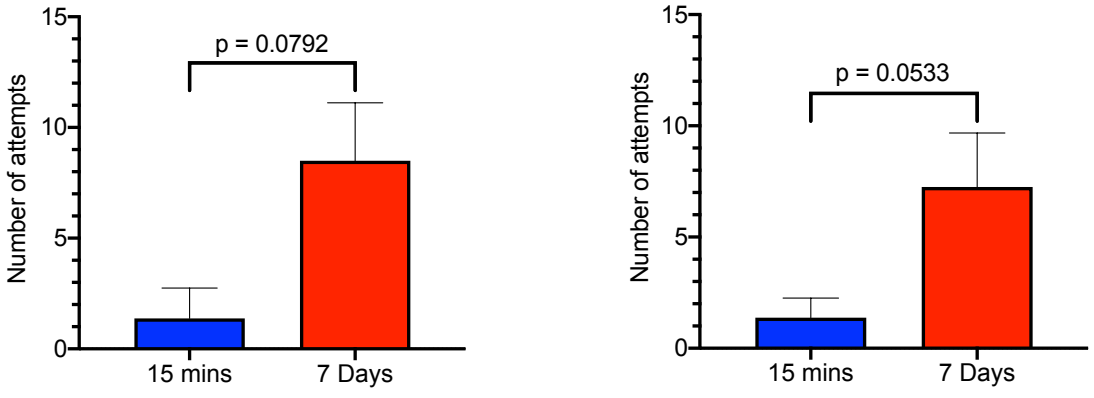


Figure 4.3: (a) Analysis of results obtained in RQ1: Comparison of the means of the number of failed login attempts after fifteen minutes and after a week with *alphanumeric authentication mechanism with no password length restriction.* (b) Analysis of results obtained in RQ2: Comparison of the means of the number of failed login attempts after fifteen minutes and after a week with *alphanumeric authentication mechanism with password length restriction.*

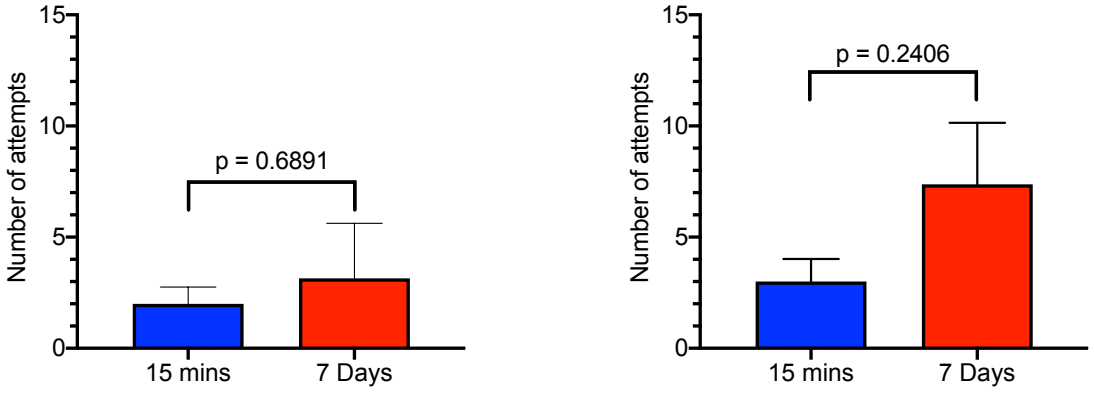


Figure 4.4: (a) Analysis of results obtained in RQ3: Comparison of the means of the number of failed login attempts after fifteen minutes and after a week with $KidsPic_{16|4}$ (b) Analysis of results obtained in RQ4 (a,b): Comparison of the means of the number of failed login attempts after fifteen minutes and after a week with *alphanumeric authentication mechanism with no password length restriction after watching an password educational video.*

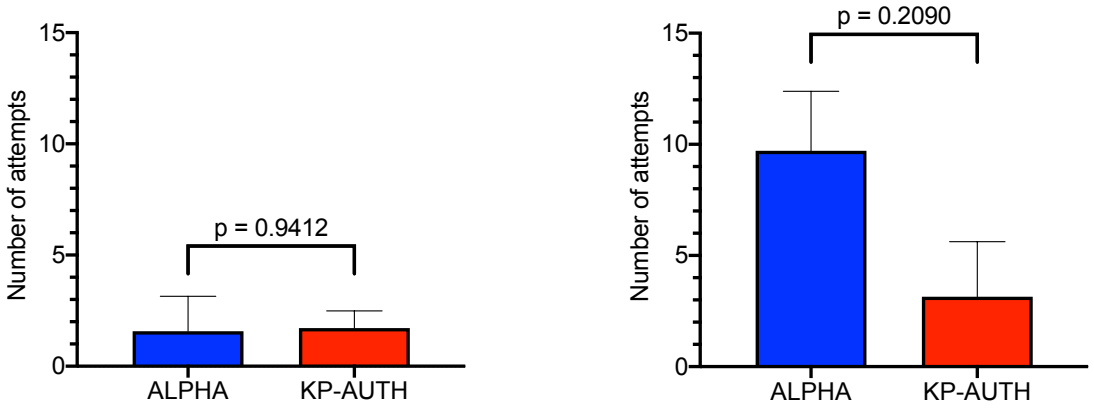


Figure 4.5: (a) Analysis of results obtained in RQ3: Comparison of the means of the number of failed login attempts for *alphanumeric authentication mechanism with no password length restriction and KP-AUTH ($KidsPic_{16|4}$)* after fifteen minutes of distraction activity. (b) Analysis of results obtained in RQ3: Comparison of the means of the number of failed login attempts with *alphanumeric authentication mechanism with no password length restriction and KP-AUTH ($KidsPic_{16|4}$)* after a week.

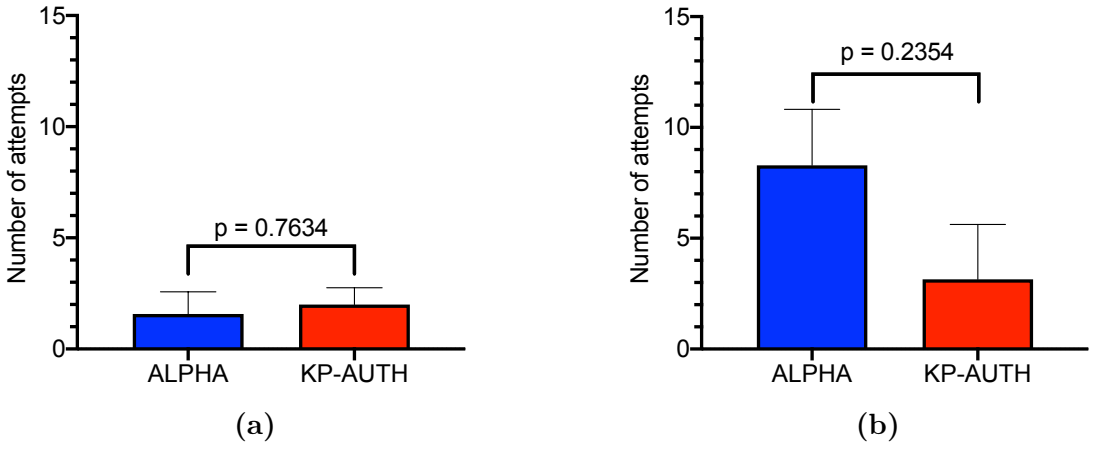


Figure 4.6: (a) Analysis of results obtained in RQ3: Comparison of the means of the number of failed login attempts with *alphanumeric authentication mechanism with password length restriction and KP-AUTH ($KidsPic_{16|4}$)* after fifteen minutes of distraction activity. (b) Analysis of results obtained in RQ3: Comparison of the means of the number of failed login attempts with *alphanumeric authentication mechanism with password length restriction and KP-AUTH ($KidsPic_{16|4}$)* after a week.

8, $\mu = 1.3$) are slightly less in comparison to KidsPic$_{16|4}$ ($n = 7$, $\mu = 2$) after playing a online game (PBS KIDS) for fifteen minutes.

In session three, children entered their usernames and passwords created from the second session — for the alphanumeric mechanism ($n = 8$; μ failed login attempts = 7.25, $p = 0.053$) as illustrated in Figure 4.3b, and for the KidsPic mechanism ($n = 7$; μ failed login attempts = 3.14, $p = 0.6891$) as shown in Figure 4.4a. Children, after watching an educational video, created an additional set of alphanumeric username and password. See Table 4.1 for alphanumeric usernames and passwords created by children. From the created usernames and passwords, we can say that, most of them did not follow the instructions given in the educational video. After playing an online game, children entered their username and password, which they created before playing a game $n = 8$, μ failed login attempts = 3.

Sessions one, two, three were conducted in the lab environment. Due to COVID-19 restrictions, we conducted the fourth session entirely online and in which children were instructed to enter their usernames and passwords remotely (from home). Researchers connected with child participants via Zoom[4] where children faced problems in entering their usernames and passwords. The collected data revealed that μ failed login attempts = 7.37 for $n = 8$, p value = 0.24 (see Figure 4.4b). Only two child participants (ages 9 & 11) entered the right set of username and password (username, password created in Session Three). As this session was conducted online and unmoderated by adult researchers, we asked children to enter their username and password when they had some free time to enter, hence the username and password entries were not exactly after a week (between 7-9 days).

[4] `https://zoom.us/`

In this chapter, we presented the results of four formative studies comparing alphanumeric and KidsPic$_{16|4,147|6,108|7}$ authentication mechanisms. During the formative studies, we increased the usability and theoretical password space of the KidsPic$_{16|4}$ authentication mechanism. The results obtained from the formative studies indicated that children were good at remembering their KidsPic$_{16|4,147|6}$ password better than an alphanumeric password in two time intervals of after fifteen minutes and after a week. With respect to RQ1 and RQ2, there were more login attempts for alphanumeric passwords (with and without restrictions) after a week compared to after fifteen minutes. This does not align with other research [10]. Children were able to remember their KidsPic$_{16|4}$ password better than their alphanumeric password (RQ3). The educational video seems to have had only a minor impact on the passwords they created (RQ4a) perhaps by using more symbols in their passwords. There were more login attempts after fifteen minutes compared to alphanumeric with and with out restrictions (RQ4b). Children were good at recognizing their chosen pictures (their password) by recalling the story they created with the pictures they selected. The formative studies conducted in the lab addressed the second over-arching research question identified in the introductory chapter that *Can children's authentication practices can be improved in terms of usability through a graphical authentication mechanism.* The results from our formative studies suggest that children were able to better remember their created password using KidsPic$_{16|4}$. As KidsPic$_{16|4}$ improved the usability (i.e. memorability in our studies), we first enhanced the KidsPic$_{16|4}$ authentication mechanism and then evaluated this enhanced version by conducting a larger usability study, both of which are described in Chapter 5.

CHAPTER 5

ENHANCING KidsPic USABILITY AND THEORETICAL PASSWORD SPACE

From the analyzed data obtained from the formative studies in Chapter 4, we found that there was no significant[1] difference in terms of the number of failed login attempts between $\text{KidsPic}_{16|4}$ and alphanumeric authentication mechanisms (see Figures 4.5a, 4.5b, 4.6a, 4.6b). However, there were more failed login attempts with the alphanumeric authentication mechanisms than with $\text{KidsPic}_{16|4}$. We also observed that children were good at remembering their picture passwords using $\text{KidsPic}_{16|4}$, both after fifteen minutes of a distraction task and after one week. The obtained results from formative studies in Chapter 4 does not align with the results from Cole et al. [10], where children had more failed login attempts with graphical authentication mechanisms compared to alphanumeric authentication mechanisms. From Chapter 4's formative studies, children were able to remember their created passwords better using KidsPic compared to alphanumeric password. We further sought to increase the usability and security of $\text{KidsPic}_{16|4}$ and to evaluate KidsPic to see if we have the supporting results for the formative studies' results.

[1] Likely in part due to the small sample size.

5.1 KidsPic Usability

Children are good at making up stories that make sense to them individually, and their story-making skills help them learn a novel thing with an ease [44]. As children are good at making up stories, using a collaborative approach researchers' encouraged and demonstrated to children how they could create a story from the pictures they selected for their $\text{KidsPic}_{16|4}$ password. When using this technique, there were no failure attempts recorded when children tried to log in after fifteen minutes and after a week. From Chapter 4, the mean of failed login attempts when using $\text{KidsPic}_{16|4}$ when not using a story to remember their password, was $\mu = 0.1428$ (after fifteen minutes) and $\mu = 0.333$ (after a week). When children created a KidsPic password with a story, the number of failed attempts was zero – after both 15 minutes and one week. The obtained results suggest that children are good at remembering their $\text{KidsPic}_{16|4}$ password with a made-up story of their choice.

Though we increased the $\text{KidsPic}_{16|4}$ *usability* by asking children to create a story with the pictures chosen by them, we did not increase its theoretical password space. For any authentication mechanism, we believe that, it is important to balance both usability *and* security. One way of evaluating the memorability/usability of an authentication mechanism is by calculating the number of failed login attempts (which we used previously). One way to evaluate the strength or security of an authentication mechanism is by calculating entropy. Entropy is the measure for a security mechanism to measure password strength. According to Hlywa *et al.*, Shannon [45, 46] the entropy can be calculated using the below Equation 5.1.

$$\log_2 (x^n) \tag{5.1}$$

$$\log_2 \left(16^4\right) = 16bits. \tag{5.2}$$

In applying 5.1 to KidsPic, x represents the number of pictures displayed in a single screen and n represents the number of screens in total. In our KidsPic$_{16|4}$ mechanism, as shown in the Figure 4.2 there are sixteen unique pictures displayed in a single screen and there are four screens in total. Hence the entropy of our KidsPic$_{16|4}$ mechanism is 16 bits (see Equation: 5.2 for entropy calculation) which is greater than the entropy of four-digit number passcode (entropy = 13.3 bits) and less than a four character alphanumeric password (entropy = 26.2 bits).

As the theoretical password space of KidsPic$_{16|4}$ in the initial series of comparison studies is relatively low, we conducted a few design sessions with an intergenerational design team composed of children ages 6-11 and adults. The design team utilized the Cooperative Inquiry method [16, 17]. The goal of the design work was to collaboratively create ways that would enhance the usability, and increase the theoretical password space and entropy of the KidsPic$_{16|4}$ authentication mechanism while hopefully still maintaining many of the memorability gains.

5.1.0.1 Design

In our design sessions using the *Cooperative Inquiry technique* [16, 17], we started the session by describing how stronger passwords are created by utilizing more diverse

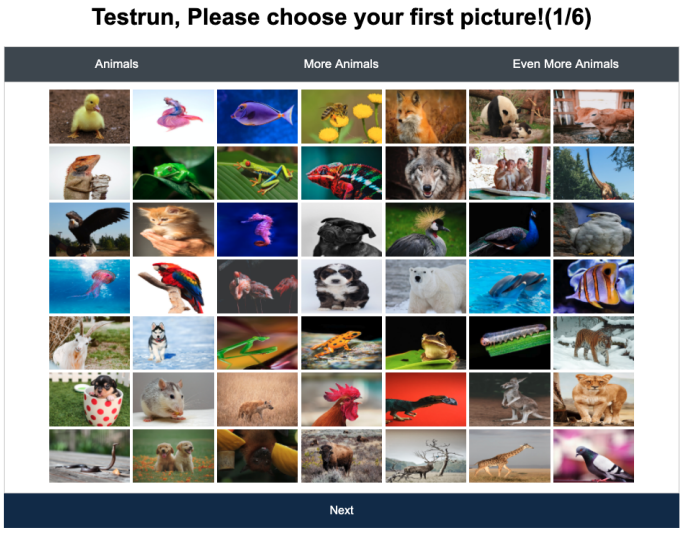


Figure 5.1: Screenshot of KidsPic$_{147|6}$ authentication mechanism displaying animal pictures with three tabs: *Animals, More Animals, Even More Animals*, each tab have a 7X7 grid of animal pictures; 147 animal pictures in total.

characters and thus increase the theoretical password space. We narrated a story *"Once upon a time there was a kid named Cody, his mom gave him two candy bags (one bag had sixteen candies and another had ninety four) and asked him not to eat them until next morning. But, Cody loves candies and failed to resist eating some candies, he ate two candies from a bag of sixteen candies and two candies from a bag of ninety four. Now a question for you all, if Cody's mom wanted to figure out which candies Cody eat, which candy bag would take more time for her to figure out which candies did Cody ate? Likewise if you choose a picture from a screen of sixteen different pictures and a picture from a screen of ninety four different pictures — which would make it easier for a hacker to figure out the picture you picked?"* Children immediately responded that a screen of ninety four different pictures would take more time or be harder for a hacker to figure out the selected picture. We

also asked children to come up with different categories of picture suggestions they would like to see in the KidsPic$_{16|4}$ authentication mechanism. Children came up with suggestions such as animals, vehicles, nature, monuments, superheroes, and emojis. After receiving suggestions from collaborative work with child design partners, we restructured the KidsPic$_{16|4}$ mechanism to include the additional pictures and categories just mentioned. The restructured KidsPic mechanism (KidsPic$_{147|6}$, see Figure 5.1) had six categories of pictures, each with 147 pictures that were displayed in three different tabs (7X7 grid of forty nine pictures in each tab).

After increasing the theoretical password space of KidsPic$_{16|4}$, the entropy increased from 16 bits (see Equation: 5.2) to 43.2 bits (see Equation 5.3) which is greater than the entropy of a six character alphanumeric authentication password (see Equation 5.4). To understand the usability of the KidsPic$_{147|6}$ mechanism, we conducted a pilot study with child design partners. The pilot study consisted of two sessions that were one week apart. In the first session, children created a username and password with KidsPic$_{147|6}$, and then played an online video game (*io Games*[2] *or PBS KIDS*) for fifteen minutes as a distraction task. After playing the game for fifteen minutes, they then logged in using the username and password they had created for KidsPic$_{147|6}$. In the second session conducted a week later, children were asked to log in again using their username and password. The goal of the pilot study was to understand the impact of the more complex password and the memorability of a KidsPic$_{147|6}$ password in two different time gaps, after fifteen minutes of a distraction task and after a week. Eight children (n = 8) created passwords in the first session and six were able to login with a single attempt after fifteen minutes of playing a

[2] `https://iogames.space/`

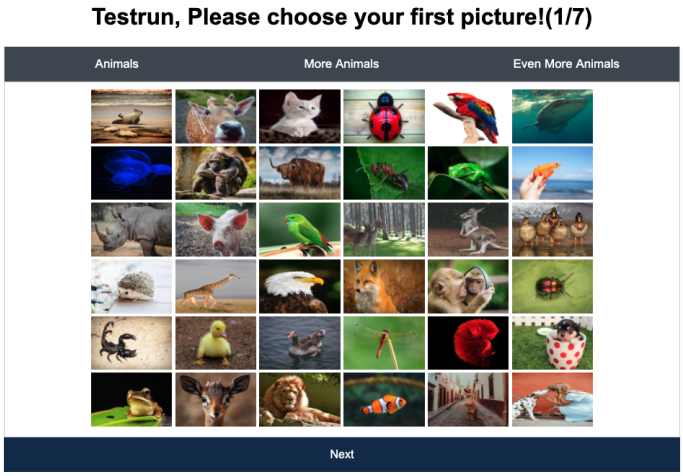


Figure 5.2: Screenshot of KidsPic$_{108|7}$ authentication mechanism displaying animal pictures with three tabs: *Animals, More Animals, Even More Animals*, each tab have a 6X6 grid of animal pictures; 108 animal pictures in total.

game (μ of failed login attempts = 0.33). At the end of the session, when we asked children about their experience with KidsPic$_{147|6}$, everyone shared their opinion about having more picture options took time to find their chosen picture during login time and, suggested us to add a *Food* pictures category. In the second session that was conducted after a week, all children (n = 7, one child was absent) were able to enter the password they had created in the first session (μ of failed login attempts = 0.14).

$$\log_2\left(147^6\right) = 43.2bits. \tag{5.3}$$

$$\log_2\left(95^6\right) = 39.4bits. \tag{5.4}$$

Based on the child participants' inputs, we modified KidsPic$_{147|6}$ by adding pic-

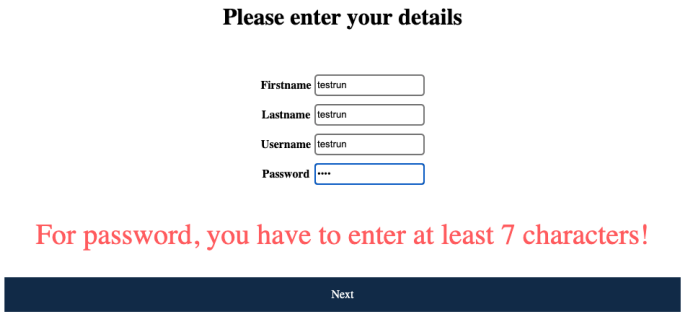


Figure 5.3: Screenshot of developed alphanumeric authentication mechanism with at least seven characters length restriction while creating password.

tures related to *food* as a seventh category. Besides adding the food category pictures, we reduced the number of pictures in each picture category from 147 to 108 (three tabs with a 6X6 grid of pictures in each tab, see Figure:5.2 ($\text{KidsPic}_{108|7}$)). By reducing the number of pictures displayed on each screen and by increasing the number of categories (screens), the resulting entropy of $\text{KidsPic}_{108|7}$ is 47.3 (see Equation 5.5 for entropy calculation), which is greater than a seven-character alphanumeric password entropy which is 46.0 bits (see Equation 5.6).

$$\log_2\left(108^7\right) = 47.3bits. \tag{5.5}$$

$$\log_2\left(95^7\right) = 46.0bits. \tag{5.6}$$

5.2 Methods Used

After modifying the ($\text{KidsPic}_{16|4,147|6}$) to better meet the usability and theoretical password space design goals, we recruited forty child participants (ages 6-11, μ age = 8.5) to conduct a usability evaluation study with $\text{KidsPic}_{108|7}$. We recruited the child participants through social media applications and through known contacts. Similar to the format of the formative studies, this usability study consisted of two sessions. Both sessions were conducted online via Zoom. The two sessions were separated by a week, and children who participated and completed both sessions received a $15 Amazon.com gift card for participating in the study. In the study, participants used two different authentication mechanisms, the mechanisms used were:

- **Alphanumeric Authentication (with password length restriction):** In this mechanism, there is a restriction for password length. Children have to create their password, which has at least seven characters (see in Figure 5.3).

- **$\text{KidsPic}_{108|7}$ Authentication:** $\text{KidsPic}_{108|7}$ is a graphical picture-based authentication mechanism in which the username is alphanumeric and the password is a set of seven unique pictures: a picture from seven categories. The categories were *Animals, Vehicles, Nature, Monuments, Superheroes, Emojis', and Food*. The pictures are displayed in three tabs and in a 6X6 grid per tab, as shown in Figure 5.2. In the registration phase, children have to select one image from each screen.

Utilizing the above-described authentication mechanisms, we addressed three re-

search questions in this usability study. Research questions in usability studies are represented as "Usability Research Questions" (URQ).

- **URQ1:** Can children remember their created username and password using an alphanumeric authentication mechanism and $\text{KidsPic}_{108|7}$ after fifteen minutes of distraction activity and after a week?
- **URQ2:** How long does it take for children to create a alphanumeric and $\text{KidsPic}_{108|7}$ username and password?
- **URQ3:** How long does it takes for children to enter their alphanumeric and $\text{KidsPic}_{108|7}$ username and password after a fifteen minutes of distraction activity and after a week?

In the first session, after receiving assent and consent from each child participant and their parent, we showed each child participant how to create an alphanumeric and $\text{KidsPic}_{108|7}$ password. Child participants were randomly assigned an order of password mechanisms (alphanumeric and KidsPic) to create usernames and passwords to minimize the potential for bias with regards to presentation order. For instance, if child participant one (CP1) was randomly assigned with $\text{KidsPic}_{108|7}$ first, after creating their $\text{KidsPic}_{108|7}$ username and password, CP1 created an alphanumeric username and password, CP2 would then use the opposite order: first alphanumeric then KidsPic. When child participants were creating their usernames and passwords, we asked them not to include passwords they were currently using to minimize the revelation of potentially sensitive information. After creating usernames and passwords, we asked child participants to play an online video game for fifteen minutes as a distraction task. Children were provided with a website link to PBS KIDS to

choose a game of their choice to play. If a child participant needed more options other than PBS KIDS, we provided them a website link to io Games and asked them to choose a game and play. After playing for fifteen minutes, children were asked to return to the main session, and were asked to enter their created usernames and passwords for each of the two mechanisms. We ended the first session by asking them a few questions about their experience with the usernames and passwords they created.

In the second session, children were asked to enter both their alphanumeric, $\text{KidsPic}_{108|7}$ usernames and passwords that they created in the first session. Children were assigned the order of the password mechanisms (alphanumeric and KidsPic) randomly. After entering their usernames and passwords to the authentication mechanisms, we concluded the second session by asking them a few questions about their experiences with usernames, and passwords.

5.3 Findings & Discussion from Usability Studies

The study consisted of forty-five child participants; five participants did not participate in the second session and so their incomplete data was excluded from the analysis. As a result, we ended up with forty participants.

Paired t-test statistical tests that compared means were used for data analysis and to determine statistical significance. A p value that is less than 0.05 ($p < 0.05$) represents a significant difference between the mean groups compared with at least 95% probability in all the mean comparisons.

Table 5.1: Responses from child participants: Age, entered alphanumeric username and passwords, the calculated alphanumeric password entropy, and calculated KidsPic$_{108|7}$ password entropy. Highlighted gray cells: Children created passwords have more entropy than KidsPic$_{108|7}$ password.

#	Age	Alpha username	Alpha password	Alpha password entropy	KidsPic$_{108\|7}$ password entropy
CP1	7	car	[child's full name]	47.0	47.3
CP2	9	Unicorn	Unicornsparle!	89.7	47.3
CP3	10	defin	ct99362	36.2	47.3
CP4	11	Flaming hot pizza	Foxers the fox	89.7	47.3
CP5	6	jasmine	cheneill	37.6	47.3
CP6	7	maine	mom1111	36.2	47.3
CP7	8	pooooooop man	1234312432	33.2	47.3
CP8	7	sundee	USAcanada	51.3	47.3
CP9	11	rainbowunicorn55555	sparklepurple	61.1	47.3
CP10	9	woodlawngirl	1234567	23.3	47.3
CP11	8	banana bird	12344321	26.6	47.3
CP12	8	dedpool123	1357924	23.3	47.3
CP13	11	lizard10	dogman001	46.5	47.3
CP14	11	DutchRoses	2009GAL	36.2	47.3
CP15	10	STRAWBERRY	PINEAPPLE	42.3	47.3
CP16	10	Ooooo	ballball	37.6	47.3
CP17	9	brok	monkeybean	47.0	47.3
CP18	7	pb	5432167	23.3	47.3
CP19	6	maxwel	5g79840	36.2	47.3
CP20	8	cookiebeast123	123457	19.9	47.3
CP21	9	quack	hi20200	36.2	47.3
CP22	9	brewster	dogsarethebest	65.8	47.3
CP23	6	Tbnr	cvvtt/u	41.2	47.3
CP24	7	ninja	pz9thebestfighter	87.9	47.3
CP25	8	kitten	uniktty	32.9	47.3
CP26	8	plasticball@	mrcatall	37.6	47.3
CP27	10	123abc	PBJ965	31.0	47.3
CP28	8	[child's fn] the great	enterthedino	56.4	47.3
CP29	6	[child's fn]	[child's mn]l87	36.2	47.3
CP30	6	blue	300298779	29.9	47.3
CP31	9	Sparkle [child's name]	[mom's phone number]	33.2	47.3
CP32	10	[child's fn]_[child's ln]123	(hello[child's fn])	58.8	47.3
CP33	11	[child's initial][child's ln]57	13905730	26.6	47.3
CP34	10	Ollie	1234567	23.3	47.3
CP35	6	sonic	sonicflash	47.0	47.3
CP36	8	[child's ln]	8818	26.6	47.3
CP37	8	[child's fn]1234	54321098	26.6	47.3
CP38	9	penguin time	eatfood	32.9	47.3
CP39	8	Fgjk	jfk	14.1	47.3
CP40	10	Tea is good	paperpen	37.6	47.3

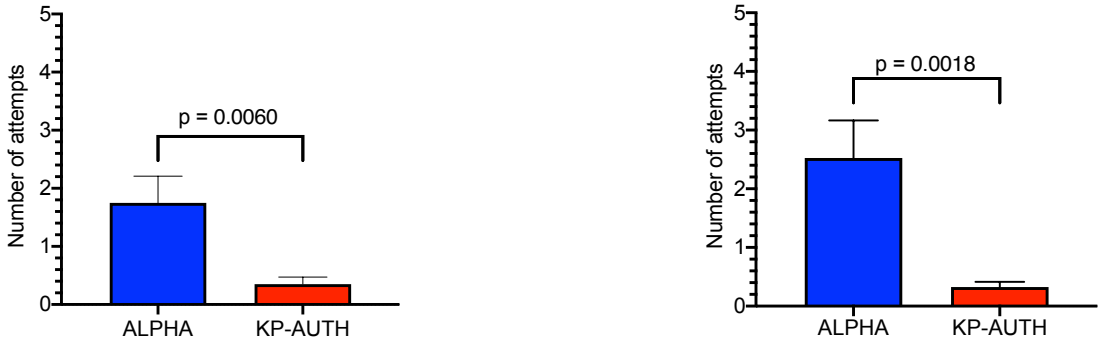
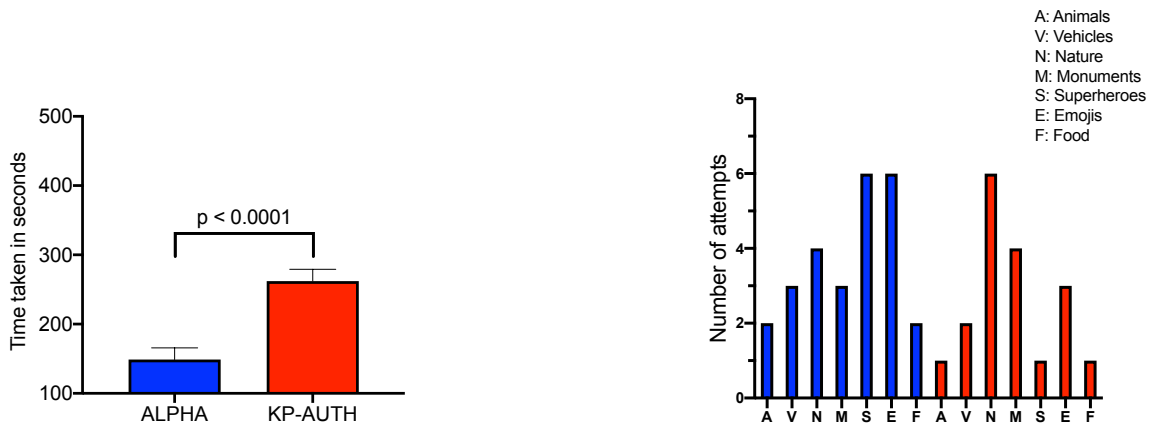


Figure 5.4: (a) Analysis of results obtained in URQ1: Comparison of the means of the number of failed login attempts with *alphanumeric authentication mechanism (with at-least seven character password length) and KP-AUTH (KidsPic$_{108|7}$)* after fifteen minutes of distraction activity. (b) Analysis of results obtained in URQ2: Comparison of the means of the number of failed login attempts with *alphanumeric authentication mechanism (with at-least seven character password length) and KP-AUTH (KidsPic$_{108|7}$)* after a week.

5.3.0.1 Failed Login Attempts

The number of failed login attempts for each participant were logged in a central database. We compared these numbers for KidsPic$_{108|7}$ and alphanumeric authentication mechanisms when children logged in fifteen minutes and one week after creating their usernames and passwords. The collected data indicated that there were more failed attempts with the alphanumeric mechanism compared to the KidsPic$_{108|7}$ authentication mechanism for both time intervals. The paired t-tests statistical analysis revealed a significant difference between failed login attempts between KidsPic$_{108|7}$ and alphanumeric authentication mechanisms. See Figures 5.4a and 5.4b for the paired t-tests results for both KidsPic$_{108|7}$ and alphanumeric with fifteen minutes and one week time intervals. The KidsPic$_{108|7}$'s failed login attempts are significantly less



(a) (b)

Figure 5.5: (a) Analysis of results obtained in URQ2: Comparison of the means number of seconds taken to create username and password during registration with *alphanumeric authentication mechanism (with at-least seven character password length)* and *KP-AUTH* ($KidsPic_{108|7}$). (b) Comparison of the number of failed login attempts with respect to each picture category. In the bar graph, blue bars indicates the count of failed login attempts after fifteen minutes and red bars represents the count of failed login attempts after a week.

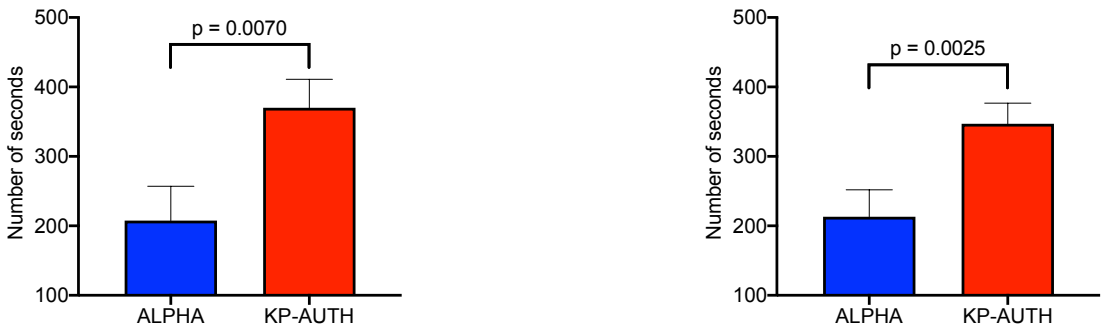


Figure 5.6: (a) Analysis of results obtained in URQ3: Comparison of the means number of seconds taken to login with *alphanumeric authentication mechanism (with at-least seven character password length) and KP-AUTH (KidsPic$_{108|7}$* after fifteen minutes of distraction activity. (b) Analysis of results obtained in URQ3: Comparison of the means number of seconds taken to login with *alphanumeric authentication mechanism (with at-least seven character password length) and KP-AUTH (KidsPic$_{108|7}$)* after a week.

compared to the alphanumeric failed login attempts which reveals a memorability advantage for KidsPic over alphanumeric passwords.

The number of failed login attempts with respect to each picture-category are illustrated in the Figure 5.5b. The failed login attempts with KidsPic$_{108|7}$ revealed that children could remember their picture of kind (for example, *" I have chosen a happy face for my emoji picture but now I see more happy faces"*). However, while selecting their picture during the login phase, they were unsure which happy face they have chosen for their password; this confusion in kids led them to have failed login attempts with KidsPic$_{108|7}$. Children were asked if the KidsPic$_{108|7}$ password was easy to remember — 85% (34 out of 40) reported that it is easy for them to remember the KidsPic$_{108|7}$ password as it is picture-based. One of the child participant mentioned that *"it's easy-peasy for me to remember this picture password."*

5.3.0.2 Password Entry Times

During the registration phase, as we expected, it took relatively more time for child participants to make their password with the KidsPic$_{108|7}$ authentication mechanism compared to the alphanumeric authentication mechanism. Please see Table 5.1 for children created alphanumeric usernames and passwords. A few child participants expressed that "it takes time to pick one picture as there are many beautiful pictures!" We recorded registration timestamps for every participant from start to finish while creating a password with both KidsPic$_{108|7}$ and alphanumeric authentication mechanisms. The paired t-test was conducted with the registration times of alphanumeric and KidsPic$_{108|7}$. Results from the paired t-test revealed a significant difference between alphanumeric registration time and KidsPic$_{108|7}$ registration time. See Figure 5.5a for the paired t-test result of the registration times.

We also expected the KidsPic$_{108|7}$ password entry during the login phase, after fifteen minutes, and after a week with to take longer for children than alphanumeric authentication mechanisms. A few child participants remembered the position of the pictures displayed during the registration phase. However, we randomized the position of the pictures when we displayed pictures during the login phase, and each subsequent login for security reasons. A few child participants expressed that they did not find their picture where they thought it would be in a screen position. The paired t-test results revealed a significant difference between alphanumeric login time and KidsPic$_{108|7}$ login times both after fifteen minutes and one week. See Figures 5.6a, 5.6b for the paired t-test result of the login times (in seconds) after fifteen minutes and after a week with respect to alphanumeric and KidsPic$_{108|7}$. As the KidsPic$_{108|7}$ has

relatively more picture options to choose and make a password, child participants took significantly more time to create a password compared to alphanumeric authentication mechanism. The pictures in KidsPic$_{108|7}$ are randomized everytime the web page is loaded, during the login phase children had to find their chosen picture and resulted in children took significantly more time to enter their KidsPic$_{108|7}$'s password compared to alphanumeric authentication mechanism.

5.3.0.3 Entropy Calculation

We calculated password entropy for both alphanumeric and KidsPic$_{108|7}$ using Equation 5.1. We encouraged children to create an alphanumeric password with at least seven characters of their choice of combinations, but there was no limit on how many characters they used. Children created their alphanumeric passwords with more than seven characters in length (see Table 5.1). Only 20% (8 out of 40) of children created alphanumeric password's entropy (see grayed out cells in Table 5.1) that was higher than their KidsPic$_{108|7}$ entropy. While the alphanumeric passwords entropy varied, the KidsPic$_{108|7}$ password entropy was constant, 47.3bits due to the way the authentication mechanism was designed (see Table 5.1).

In this chapter, we conducted usability studies with a larger sample size and with enhanced KidsPic$_{108|7}$ authentication mechanism and the obtained results are supporting the formative studies results from *Chapter 3*. The KidsPic$_{108|7}$ authentication mechanism improved the usability and security aspects which addressed one of the primary research questions: *Can children's authentication practices be improved in terms of security and usability through a graphical authentication mechanism.*

Though the KidsPic$_{108|7}$ authentication mechanism is more usable and secure than the alphanumeric authentication mechanism used in our evaluation studies, the time taken for children to create and login using KidsPic$_{108|7}$ authentication mechanism is significantly more compared to the alphanumeric authentication mechanism. On the other hand, the number of failure login attempts with KidsPic$_{108|7}$ authentication mechanism are significantly less compared to the failure login attempts with alphanumeric authentication mechanism.

Due to the COVID-19 pandemic, our daily lives have been dramatically changed which has impacted our research too. The pandemic required that the four formative studies and the larger usability study be conducted completely online. Though technology helped us to recruit and conduct studies with child participants, there are a few limitations using technology. We experienced some technological limitations including weak internet connections and the devices which children used for the study were not working correctly which led to rescheduled sessions, etc. We recruited forty five child participants for the usability study and, out of forty five, five child participants did not participate in the second session — as a result we did not consider their data in our analysis. Since KidsPic took children more time to create and login with than the KidsPic$_{108|7}$ authentication mechanism, we would like to see if that time can be reduced and whether that time is part of the influence that helps children more readily remember their password.

CHAPTER 6

INVESTIGATING ADDITIONAL ASPECTS OF GRAPHICAL AUTHENTICATION

From the findings obtained in Chapter 5, I identified several elements needing further research identified as research objectives that are outlined in this section. Though the KidsPic$_{108|7}$ authentication mechanism increases the theoretical password space by increasing the number of pictures in each category, the results from our preliminary research identified some scenarios where the same picture (from the set of 108) was selected by different child participants for their passwords (see Figure 6.1). While this is always a possibility, it is imperative to understand why and how often this occurs as the increased theoretical password space is a primary strength of KidsPic$_{108|7}$. Many duplicate selections would weaken the strength of KidsPic.

In this chapter, we identify and list the research objectives associated with further understanding and improving the usability and security of KidsPic which align with my primary research questions identified in the introductory chapter (Chapter 1). The below research objectives (RO) helped me understand more about children's picture selection preferences in terms of usability and theoretical password space utilization of KidsPic$_{108|7}$. Hence, the below-described research objectives are divided into two

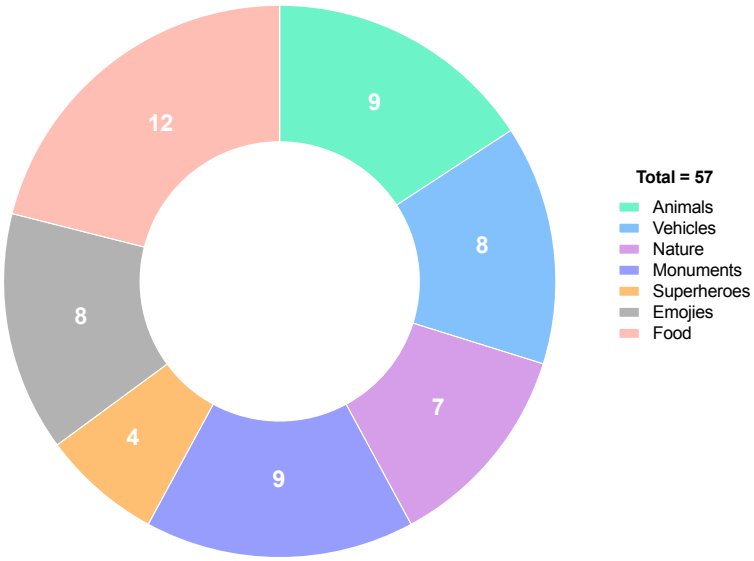


Figure 6.1: Pie chart depicting the number pictures chosen by more than one child participants for their passwords in each picture category.

main groupings — one group consists of research objectives which will help me to understand and increase the usability of KidsPic$_{108|7}$ (RO1-5), and the other will allow me to incorporate additional security features into KidsPic (RO6-8).

- **RO1:** Does picture resolution impact children's picture selection?
- **RO2:** Does altering (modifying) categories of pictures increase password memorability?
- **RO3:** Does the number of objects in a single picture influence children as they choose a picture for their password?
- **RO4:** What picture features are correlated between those selected for passwords among all participants?

- **RO5:** How do we limit the number of failed login attempts (to avoid the brute-force attacks on KidsPic) and how does that impact children's ability and motivation to complete their password?

- **RO6:** How to avoid *shoulder surfing* attacks in KidsPic?

- **RO7:** How guessable are children's passwords by someone close to them?

In the following sections, the above-mentioned research questions (RO1-RO7) are explained in further detail. To address these questions, differing methods were used to achieve the varied research objectives. These methods included participatory design sessions with children and adults, as well as usability evaluation studies. ***Participatory Design Sessions (RO2-RO4)*** were conducted within our lab's intergenerational team (Kidsteam), where children and adults work together to design technologies for children [16, 17]. The Kidsteam I worked with in this research consisted of ten children ages 6-11 and several adult researchers. ***Usability Evaluation Studies (RO1, RO5-RO7)*** were conducted to understand the designed prototypes with children ages 6-11 by recruiting from the United States. Children evaluated the designed prototype in the usability evaluation studies and shared their feedback with adult researchers.

6.1 RO1 (Protocol 1): Investigating if Resolution of Pictures Influence Children to Choose a Picture for their Password

6.1.1 Overview

The data from Chapter 5 revealed that multiple child participants chose specific pictures within categories. The ramifications of this duplicate selection are that children are not utilizing the entire theoretical password space to choose their password picture in each category, thus potentially weakening the strength of KidsPic. In other words, though there are multiple "cat" pictures to choose from within the "Animals" category, a few children chose "a cat picture" for their animal picture, and duplicate pictures were selected.

6.1.2 Participants Recruitment

As this research objective is more of a design exploration, I conducted this design exploration study within our lab's intergenerational team (Kidsteam), where children and adults work together to design technologies for children [16, 17]. Kidsteam currently has ten kids ages 6-11 and several adult researchers.

6.1.3 Methods Used

To understand whether children are influenced by the resolution of the pictures while choosing pictures as their passwords, I conducted a participatory design session.

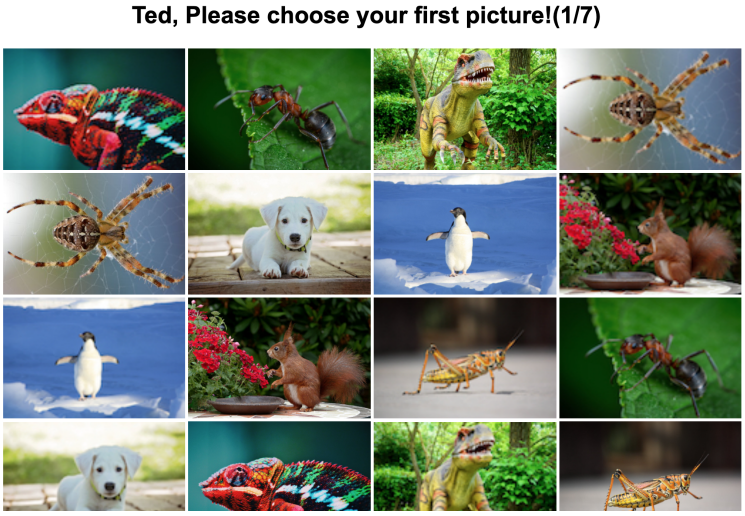


Figure 6.2: A version of KidsPic$_{16|7}$ with eight better quality and eight reduced quality pictures.

6.1.4 KidsPic$_{16|7}$ Design

From my preliminary research studies (ages 6-11, n=40), we observed some instances where different child participants selected the same pictures for their passwords. One hypothesis for this duplication was that there might be a chance children were being influenced by the quality of pictures. The aspect ratio and resolution are a couple of factors that can determine the quality of a picture. I designed a different version of the KidsPic$_{16|7}$ authentication mechanism to test this research hypothesis (RO1). In this version, there are 16 pictures displayed on each screen for each category; and in total, there are seven categories (Animals, Vehicles, Nature, Monuments, Superheroes, Emojis, Food). In other words, children have to select a picture from each category, and a total of seven pictures is their password. There are only eight unique pictures (367X244 pixel dimensions) in each picture category, and

the remaining eight are the reduced quality (128X85 pixel dimensions) of those unique pictures (refer to Figure 6.2). To avoid bias, selecting the original eight unique pictures in all the picture categories was completely randomized. All pictures are randomly distributed in a four-by-four grid. The purpose for asking children to choose pictures from this modified KidsPic was to see which quality (better or reduced quality) of the picture they would prefer for their password.

6.1.5 Study Procedure

This usability study aims to understand the effect of pictures' quality on drawing children to select those images for their passwords. To achieve this goal, I conducted a participatory design session with Kidsteam (n=8) and utilized the $\text{KidsPic}_{16|7}$ password mechanism. After introducing the purpose of the participatory design session, child participants were divided into four groups; in each group, an adult researcher facilitated two child participants. After children joined the breakout rooms, they created usernames and passwords using $\text{KidsPic}_{16|7}$. After password creation, children played an online video game for distraction purposes; in other words, to see if they would remember their pictures, including quality, after playing an online video game as a distraction activity. After playing an online video game, children returned to the system ($\text{KidsPic}_{16|7}$) to enter their created passwords. Children entered their usernames and passwords; password hints were provided by the adult researchers if necessary. We concluded the participatory design session by asking children a few questions about their password selection during the registration phase. The adult researchers' took notes and filled out survey responses for children from each group.

Table 6.1: Child participant's age, and their image quality choice from each category during registration phase. "H" indicates better quality and "L" indicates reduced quality pictures.

#	Age	Animals	Vehicles	Nature	Monuments	Superhero	Emoji	Food
P1	08	H	H	H	H	H	H	H
P2	09	L	H	H	L	L	L	L
P3	09	H	H	H	H	H	H	H
P4	09	L	L	H	L	H	H	L
P5	11	H	L	H	H	L	L	H
P6	11	L	H	L	H	L	L	L
P7	11	L	H	L	L	L	L	L
P8	11	H	H	L	H	L	L	H

6.1.6 Results and Analysis

Both children's registration and login attempts were recorded in a central database, including their picture choices. The survey responses were collected and stored via the Qualtrics survey tool. The rest of this section will discuss the collected results concerning children's choice in selecting better or reduced-quality pictures and memorability in remembering their password including quality after playing an online video game. From the collected registration data, on average, children selected 3.75 pictures with better quality and 3.25 pictures with reduced quality. It is interesting to observe from the registration data that two child participants (P1, P3, ages 8 and 9) chose all better quality pictures from all picture categories for their $\text{KidsPic}_{16|7}$ password. Please refer to Table 6.1 for the pictures that the child participants chose, as well as their age.

The qualitative data collected from the surveys indicate that children chose pictures purely based on their association. After playing the online video game, when

children tried to enter their created password, all the child participants were able to remember the content in the picture but not the quality of the picture they chose during the registration phase. Two child participants were able to remember the quality of pictures too; ages 8 and 9 and they both support no influence based on resolution. From the quantitative analysis of collected results we observed no significant difference between choosing a number of better and reduced-quality pictures for child passwords. The survey responses by child participants from our study indicated that children did not choose pictures for their passwords by picture quality/resolution but only by their association with the content of the pictures. From the analysis of both qualitative and quantitative data, it is clear that children choose their pictures for their password purely based on their association with them and not depended on the picture resolution.

6.2 RO1: Protocol 2

From Protocol 1 in this research objective, we observed no influence in children regarding the quality of pictures while selecting their passwords. As there is no significant difference observed between better and reduced quality pictures, we decided to alter the design and follow the same study procedure as protocol 1 to observe if the modified protocol would produce the same results. In this protocol, we replaced pictures from better to reduced and reduced to better quality in this protocol. In other words, if the child participant selected a better quality picture during the registration phase, the better quality picture is replaced with reduced quality of pictures during the login phase.

6.2.1 Participants Recruitment

As this research objective is more of design exploration, I conducted this design exploration study within Kidsteam.

Figure 6.3: A version of KidsPic$_{16|7}$ with 16 unique pictures randomly displayed in a grid with a combination of eight better quality and eight reduced quality pictures.

6.2.2 Methods Used

To understand whether children are influenced by the resolution of the pictures while choosing pictures as their passwords, I conducted a participatory design session.

[0]https://kidsteam.boisestate.edu/FROQ1_P2/reg_1.php

6.2.3 KidsPic$_{16|7}$ Design

To evaluate this research objective, I designed and developed a different version of the KidsPic authentication mechanism with 16 pictures for each category, and there are seven screens in total, with each category per screen. In other words, children have to select a picture from each screen, and a total of seven pictures is their password. Each screen has 16 unique pictures from each picture category (refer to Figure 6.3), among 16 pictures; eight are better quality pictures, and the remaining eight are low-quality pictures. Sixteen unique pictures are selected randomly in all seven picture categories. To differentiate the quality between pictures in each category of pictures, I used two different pixel dimensions. The better quality pictures have 367X244 pixel dimensions, and the low-quality picture pixel dimensions are 128X85. The idea is to present both better and low-quality pictures in each category to children and observe if children would pick a better or low-quality picture from their picture selection for their passwords. During login, the quality of the chosen picture is replaced by alternate picture quality; for example, if a participant has chosen a cat picture with low picture quality during the registration phase, it is replaced with a better quality picture during login phase.

6.2.4 Study Procedure

This study aims to understand the effect of picture's quality on drawing children to select those images for their passwords. I conducted a participatory design session with Kidsteam (n=6) and utilized KidsPic$_{16|7}$ password mechanism to achieve this goal. After introducing the purpose of the participatory design session, child partici-

Table 6.2: Child participant's age, and their image quality choice from each category during registration phase. "H" indicates better quality and "L" indicates reduced quality pictures.

#	Age	Animals	Vehicles	Nature	Monuments	Superhero	Emoji	Food
P1	09	H	H	H	H	L	L	H
P2	09	L	H	L	L	H	L	H
P3	10	H	H	H	H	H	L	H
P4	11	L	L	L	L	H	L	L
P5	11	H	L	L	L	L	L	H
P6	11	L	H	L	L	H	L	H

pants were divided into four groups; in each group, an adult researcher facilitated child participants. Children created usernames and passwords using KidsPic$_{16|7}$. Followed by children played an online video game which helped us to see if children can remember their chosen pictures with their quality. After playing an online video game, children returned to the system (KidsPic$_{16|7}$) to enter their created passwords. Children entered their usernames and passwords; password hints were provided by the adult researchers if necessary. We concluded the participatory design session by asking children a few questions concerning their password selection during their registration phase. The adult researchers' took notes and filled survey responses for children from each group.

6.2.5 Results and Analysis

Both children's registration and login attempts were recorded in a central database. The survey responses were collected and stored via the Qualtrics survey tool. The rest of this section will discuss collected results concerning children's choice in selecting better or reduced-quality pictures and memorability in remembering after playing an

online video game. From the collected registration data, on average, children selected 3.34 pictures with better quality and 3.67 pictures with reduced quality. Unlike the other protocol results, it is interesting to observe from the registration data that no child participants chose all better or low-quality pictures from all picture categories for their KidsPic password.In other words, child participants chose a mixture of both better and low-quality pictures for their passwords. Please refer to Table 6.2 for the complete distribution of pictures chosen by all child participants with their ages.

The collected data from the surveys indicate that pictures were chosen by children are seemingly based on their association with content of the chosen pictures. After playing the online video game, when children tried to enter their created password, all the child participants could remember the content in the picture but not the quality of the picture they chose during the registration phase. **The obtained results in this study protocol are completely aligned with protocol 1's results**. We observed no significant difference between children choosing both better and low-quality pictures for passwords. From analysis of the survey responses indicates us that child participants from our study did not choose pictures for their passwords based on the picture quality/resolution but only by their association with the content of the pictures. From the analysis of both qualitative (survey responses) and quantitative (average number of better/reduced-quality pictures) data, it is clear that children choose their pictures for their password using KidsPic is purely based on their association with pictures and not depended on the picture resolution.

6.3 RO2: Modifying the *Type* or *Order* of the Picture Categories

6.3.1 Overview

The data from Chapter 5, revealed that multiple child participants chose specific pictures within categories. Results from our investigation into URQ1 from Chapter 5 indicated significantly fewer failed login attempts with KidsPic than the alphanumeric authentication mechanism. Though there are fewer failed login attempts for KidsPic, children were not utilizing the complete theoretical password space of KidsPic. For instance, multiple child participants chose the same pictures for their password; therefore, duplicate pictures were chosen. Understanding the child participants' preference in choosing pictures in terms of a different order of the picture categories displayed for children to select their password lead us to determine if the change in the order of picture categories may reduce the selection of duplicate pictures.

6.3.2 Participants Recruitment

No participants were recruited. Since this research objective is more of design exploration, I worked with Kidsteam child participants (ages 6-11, n=6).

6.3.3 Methods Used

To achieve this research objective, I conducted a participatory design session for understanding the children's picture preferences while creating their picture pass-

words, if children prefer to change the order of categories for the KidsPic authentication mechanism.

6.3.4 Study Procedure

To address this research objective, I designed an interactive Qualtrics survey[1]. The survey consists of a set of pictures, and to avoid bias, pictures were chosen randomly from each category. Children were first asked to re-order the pictures according to their preferences, make a story for each set of re-ordered pictures, and explain why they chose that order. We aimed to complete this study in a single session, and all the child participants' responses were collected and stored in the Qualtrics survey tool.

The participatory design session's results helped us understand that the child participants are good with the current order of picture categories for KidsPic. In addition, the order of picture categories will support children's cognitive ability in making stories to remember the chosen pictures. The results from the participatory design sessions align with the observations from the preliminary research studies (n=40). This current study aims to understand children's preferences pertaining to the sequence of pictures when creating a password using the KidsPic authentication mechanism. The current KidsPic authentication mechanism's picture category order is Animals, Vehicles, Nature, Monuments, Superheroes, Emojis, and Food. We performed a participatory design sessions with Kidsteam (n=6) to seek their input on changing the order of the picture categories. After introducing the purpose of the participatory design session, child participants were divided into three groups;

[1]https://boisestate.az1.qualtrics.com/jfe/form/SV_6zCIhENtghqSRRc

Table 6.3: The table represents the analysis of the survey data where children reordered the picture categories. The highlighted cells with gray color indicate that the majority of the child participants would like to have that category in the respective position (from first column) for the KidsPic authentication mechanism. For instance four child participants would like to have Animals as the first category for the KidsPic authentication mechanism.

Position	Animals	Vehicles	Nature	Monuments	Superhero	Emoji	Food
First	4	1	1	0	0	0	0
Second	0	4	0	1	0	0	1
Third	1	1	4	0	0	0	0
Fourth	0	0	0	5	1	0	0
Fifth	0	0	0	0	5	0	1
Sixth	1	0	1	0	0	4	0
Seventh	0	0	0	0	0	2	4

in each group, an adult researcher facilitated two child participants. I designed an interactive Qualtrics survey with a picture from each category randomly distributed and asked them to change the order to their preferred order. Children interacted with the Qualtrics survey tool and completed the survey. After reordering the pictures, we concluded the participatory design session by asking children a few questions concerning their opinion on different order of picture categories in KidsPic.

6.3.5 Results and Analysis

The survey responses were collected and stored via a Qualtrics survey. The rest of this section will discuss collected results about children's priority in choosing an order for picture categories. More than fifty percent of the child participants wanted the same order of picture categories for the KidsPic authentication mechanism from the collected survey data. Please refer to Table 6.3 for the complete distribution

of pictures chosen by all child participants. We assume that child participants are familiar with the picture categories' current order, which led them to choose the same order.

The observations from the collected data explain that most of the child participants want to have the existing order of the picture categories. Although, interestingly, two-child participants (ages 8,11) mentioned that they "would like to have hard picture categories at the first and easy picture categories at last." Though their opinions are the same, the hard and easy picture categories were different for each of them.

6.4 RO3: Multiple Objects in a Single Picture

6.4.1 Overview

In $\text{KidsPic}_{108|7}$ mechanism, there are pictures with more than one object in them (see Figure 6.4a, 6.4b). The one hypothesis was whether the number of objects in a picture influenced or not while selecting those pictures for their password. To achieve this goal, I utilized the data from URQs (from Chapter 5) which could lead to interesting observations.

6.4.2 Participants Recruitment

No participants were recruited. The data collected from Chapter 3 was used for analysis.

(a)

(b)

Figure 6.4: (a) Represents a picture which has more than one objects in *Animals* category in KidsPic$_{108|7}$ (b) Represents a picture which has more than one objects in *Vehicle* category in KidsPic$_{108|7}$

6.4.3 Results and Analysis

The aim of this research objective was to obtain the total number of objects from each picture from the picture repository used to achieve the URQs in Chapter 5. The data consists of pictures chosen by 40 child participants during the registration phase and the pictures which are not chosen by the child participants. For extracting the total number of objects from each picture, I wrote a Python script and integrated it with Google Vision API [2] to extract the total number of objects from each picture in the picture repository for the KidsPic authentication mechanism and stored the extracted objects in a centralized data table. Using the Google Vision API, I was able to avoid any human bias for obtaining a number of objects from each picture.

[2]https://cloud.google.com/vision

Figure 6.5: A "Food" picture used in the KidsPic$_{108|7}$ with 14 donuts in the picture.

Though the Google Vision API helped to extract the objects from all the pictures, the extracted objects often consisted of duplicates. There were inconsistencies in including the duplicate objects from each picture. To simplify the data, duplicates were removed as the focus was on object counts. For instance, see Figure 6.5, the picture consists of 14 donuts, and Google Vision API generated the count as 10; in removing the duplicates, the count of unique objects in the donuts picture is one. We also normalized the data to compare the average number of objects found in each picture category (as some categories seemingly had more objects than others). To compare, I computed delta by subtracting the total number of unique objects from the average number of objects in that picture category for each picture.

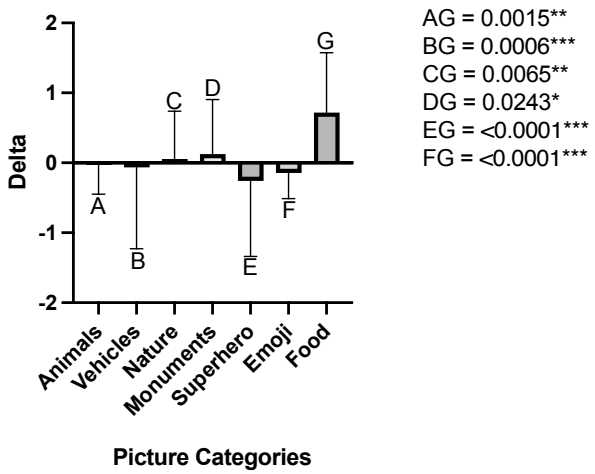


Figure 6.6: Average number of objects in the picture category selected by child participants using $\text{KidsPic}_{108|7}$. Also, we can observe a significant difference between the average number of objects from each picture category with the "Food" picture category.

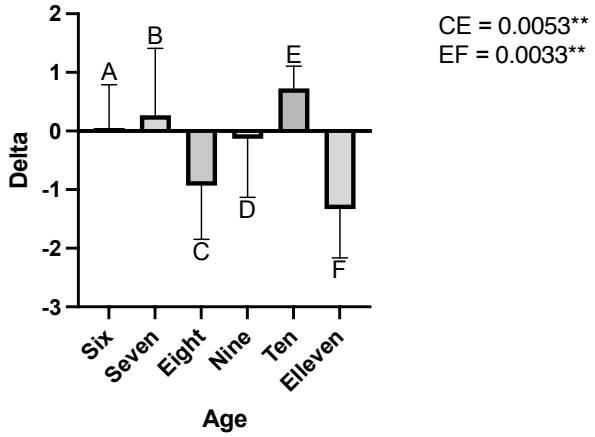


Figure 6.7: Average number of objects from superhero picture category with respect to child participants' age groups using $\text{KidsPic}_{108|7}$. We can observe a significant difference between (eight(C), ten(E)) and (ten(E), eleven(F)) age groups.

We performed both descriptive and statistical regression analyses on the data collected, normalized data set. We utilized the one-way Anova method to compute and observe the statistical deference between multiple independent variables. Figure 6.6 represents the bar graph that compares the delta's mean of objects in pictures which were selected by the 40 child participants for their KidsPic password. In Figure 6.6, we can observe that there are significantly more objects present in the "Food" picture category compared to other picture categories. We think the observed significant difference is because the "Food" picture category has more objects in each picture compared to pictures in other categories. As the child participants are in the age group of 6-11, another interesting insight was to see if there is a significant difference in the number of objects in pictures chosen by child participants in each picture category between different age groups. Except for the "Superheros" picture category, we did not observe a significant difference in the number of objects in pictures that children selected in different age groups (refer to Figure 6.7). From the analysis, the number of objects present in each picture that children selected did not influence children to choose pictures for their password. Child participants have chosen pictures for their passwords purely with their association with the pictures but not dependent on the number of objects in each picture.

6.5 RO4: Extracting Picture Features and Drawing Correlations from the Collected Data

6.5.1 Overview

An in-depth analysis of pictures that the child participants chose during the registration phase of $\text{KidsPic}_{108|7}$ can give us insights that can help us understand the picture preferences. Extracting picture features can help us correlate and understand the children's picture preferences. The Google Vision API can extract the picture features like dominant colors and the total number of objects in each picture. In this research question, I used Google Vision API to extract the dominant colors from each picture in the pictures' database used for $\text{KidsPic}_{108|7}$. In this research question, I explored patterns relative to the dominant colors of the pictures that the children selected when creating their passwords.

6.5.2 Participants Recruitment

No participants were recruited. The collected data from Chapter 3 was used for analysis.

6.5.3 Methods and Study Procedure

To achieve this research goal, the data/results from URQ1, URQ2, URQ3 in Chapter 5 were used to extract picture features. I analyzed the collected registration data from chapter three. To extract different dominant colors from pictures, I wrote

a code snippet in Python and integrated it with the Google Vision API to extract the dominant colors from pictures. Colors were then put into 16 HTML4 color categories[3].

Figure 6.8: The picture depicts the end screen of the login phase in KidsPic$_{108|7}$. The end screen displays the pictures of who logged into the KidsPic$_{108|7}$.

6.5.4 Results and Analysis

The Google Vision API extracted ten dominant colors for each picture (see Figure 6.8). The extracted dominant colors are represented in hexadecimal values. As the front-end of the KidsPic$_{108|7}$ was developed in HTML4, I converted the hexadecimal into HTML4 color codes using the python script. There were sixteen unique HTML4 colors extracted and are listed in Table 6.4. There were many pictures with duplicate HTML4 colors among the extracted ten dominant colors; for instance, black can be repeated twice. I cleaned the data by summing the duplicate colors in the extracted dominant colors; for example, a picture can have black color repeated twice. The Google Vision API produces two different percentages of black color. In the process

[3]https://en.wikipedia.org/wiki/Web_colors

Table 6.4: Table depicts the 16 unique HTML4 colors with their hexadecimal codes and their names.

HTML4 Hexadecimal Code	Color
000000	Black
C0C0C0	Silver
808080	Gray
FFFFFF	White
800000	Maroon
FF0000	Red
800080	Purple
FF00FF	Fuchsia
008000	Green
00FF00	Lime
808000	Olive
FFFF00	Yellow
000080	Navy
0000FF	Blue
008080	Teal
00FFFF	Aqua

of removing duplicates, I added the two percentages of any repeated colors to have all unique colors for the pictures used in the $\text{KidsPic}_{108|7}$.

I performed both descriptive and statistical regression analyses with the data collected from Google Vision API. The results from the analysis suggested that there is no pattern relative to the dominant colors of the selected pictures by child participants when creating their passwords. We observed from the collected data analysis that the child participants did not choose pictures for their picture password with similar dominant colors as they progressed from Animal to Food and through all picture categories.

6.6 RO5: Avoiding *Brute-Force* Attack on KidsPic$_{108|7}$

6.6.1 Overview

The collected data from Chapter 5 indicated that the average number of failed login attempts is two. The current version of KidsPic$_{108|7}$, which we used in the in Chapter 5, does not have any restrictions for children on the number of failed login attempts – meaning they can keep on trying to enter the correct password over and over again. No restrictions on the number of attempts for entering a password using KidsPic$_{108|7}$ may lead to a security attack called a *brute-force attack*. To avoid brute-force attacks on KidsPic, a common approach is to limit the number of login attempts for a user within a specific window of time, and further attempts would prompt either a delay in trying again or locking the account. It is interesting to investigate how this restriction impacts the usability of KidsPic in terms of children's motivation to complete entering their password.

6.6.2 Participants Recruitment

The aim of this research objective was to design a mechanism to mitigate brute-force attacks on the KidsPic authentication mechanism. We conducted a participatory design session with Kidsteam children as this research objective is more design-related.

6.6.3 Methods Used and Study Procedure

In one of the design sessions with Kidsteam, using cooperative inquiry techniques, we asked children to design an approach to mitigate brute-force attack. The outcomes of this design session are not only KidsPic with limited login tries in a given time, but also the Kidsteam designed ideas to mitigate a brute-force attack in KidsPic.

6.6.4 Results and Analysis

During the participatory design session, I introduced the concept of a brute-force attack to children. Children then worked with adults in smaller groups (in breakout groups in Zoom) to design a mechanism that could avoid the brute-force attack in the KidsPic authentication mechanism. Several different ideas emerged from this participatory design session.

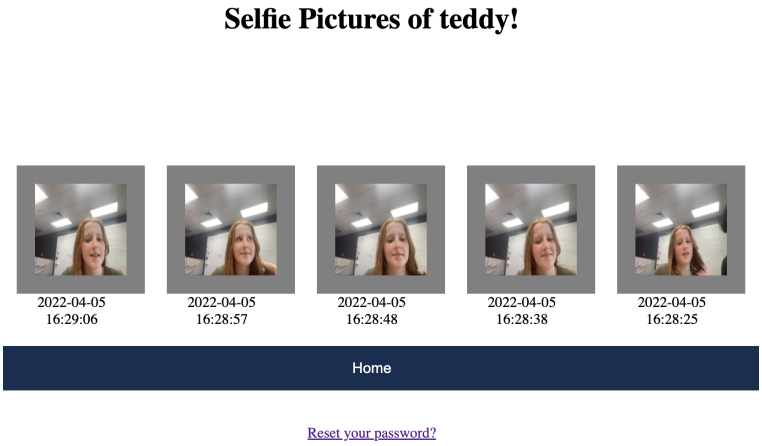


Figure 6.9: The picture depicts the end screen of the login phase in KidsPic. The end screen displays the pictures of *teddy* (username) logged into the KidsPic.

Many of the children-inspired designs obtained during the participatory design session were inspired by biometric authentication mechanisms; for example integrating fingerprint authentication to avoid brute-force attacks. Another big idea we pursued and I implemented from the participatory design session was "to take a picture of the person who logged into the account and displays the taken pictures after a user logged in". As such, I developed and integrated the picture-taking mechanism in the KidsPic authentication mechanism that displays the pictures with the timestamp of the person who logged in to the account of the last five login attempts (see Figure 6.9). Using this feature, users can see who has been logged in to their account during the previous five attempts. Some of the systems use something similar e.g. CentOS[4] but CentOS just logs username and timestamp. If they notice any suspicious login attempts, they can change their username and password immediately. We mitigated the Brute-Force attack on the KidsPic authentication mechanism by implementing the picture-taking mechanism with timestamp displaying for children whenever they login to their accounts.

6.7 RO6: Avoiding Shoulder Surfing Attack on KidsPic$_{108|7}$

6.7.1 Overview

To increase the usability of the KidsPic authentication mechanism, upon completing the registration phase of choosing the sequence of seven pictures, all pictures are displayed on a final screen to allow them to review their pictures and create a story with them. While this helps children recall their picture selections later, this

[4]https://www.centos.org/

presents a vulnerability to a common security threat: a shoulder surfing attack. A shoulder surfing attack occurs when someone looks over your shoulder and sees your password as you enter it. When a user is trying to log in to the system using his credentials and being watched from behind by someone to obtain his credentials is called a shoulder surfing attack. It is important for any security measure to strive to mitigate the shoulder surfing attack for KidsPic.

6.7.2 Participants Recruitment

This research objective was to explore ways to avoid shoulder surfing (and not to explicitly compare two mechanisms). This research question was investigated via a design exploration with Kidsteam.

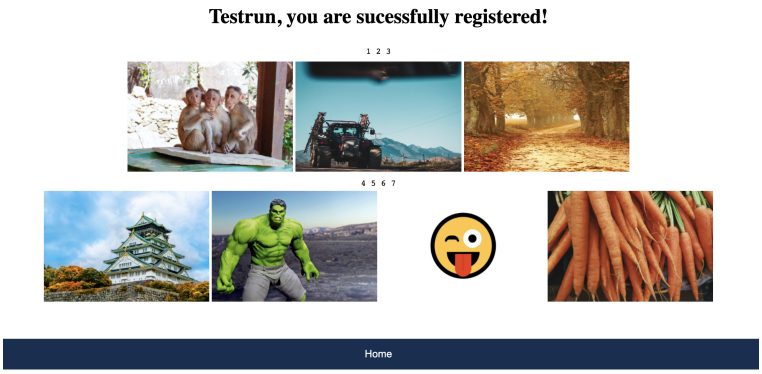


Figure 6.10: Pictures displayed in a sequence in the end screen after registration is complete using KidsPic$_{108|7}$.

6.7.3 Methods and Study Procedure

The KidsPic$_{108|7}$ used in Chapter 5 has no measures to avoid shoulder surfing attacks. Besides, pictures selected by child participants are displayed in a sequence (see Figure 6.10) at the end screen. The only purpose of displaying the pictures in a sequence at the end screen is to help the child participants remember their chosen pictures and make a story seeing them (pictures). The end screen for KidsPic$_{108|7}$ is prone to shoulder surfing attacks as it contains the child participant's complete password in order to unblur them and review their password and revisit their password story.

To collaboratively find ways to avoid the shoulder surfing attack for the KidsPic authentication mechanism with children, I led a participatory design session with Kidsteam. In this design session, I first helped children understand what a shoulder-surfing attack is and how the KidsPic authentication mechanism is susceptible to such attacks. After discussing what a shoulder surfing attack was, children quickly understood the importance of safeguarding their credentials from this vulnerability. Children were then asked to help design solutions to avoid (or minimize the potential of) a shoulder surfing attack on KidsPic. The Kidsteam came up with some ideas like "covering up the entire with black color and revealing the password upon entering a numeric four-digit passcode."

I developed and integrated a mechanism that avoids the shoulder surfing mechanism into the KidsPic authentication mechanism from the ideas that children shared by the child participants in the participatory design session. The developed mechanism that avoids the shoulder surfing attack will blur the pictures chosen by the

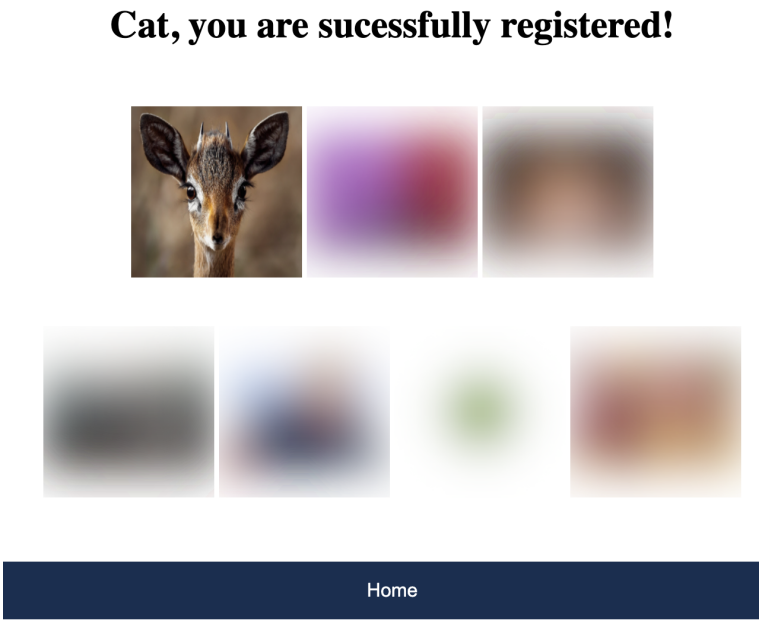


Figure 6.11: Pictures displayed in a sequence in the end screen after registration is complete using KidsPic$_{108|7}$. Animal picture is unblured as child participant hovered on it. The rest of the Pictures of their password are blurred to protect their password from shoulder surfing attack.

child participants and are displayed on the end screen of the KidsPic authentication mechanism; by doing so, the person from over the user's shoulder can not see the pictures that the user chose. If children want to view their pictures for reference, they can click/hover on each picture to unblur that particular picture of their password (see Figure 6.11). To avoid the shoulder surfing attack effectively, the mechanism will unblur only for 50 milliseconds when it is hovered/clicked; after 50 milliseconds, the pictures will get blurred again. In one of the Kidsteam participatory design sessions, I collected children's opinions on the shoulder surfing mechanism integrated with KidsPic. All the child participants liked the idea of blurring the pictures so that a person standing over the shoulder could not look at their password. At the same

time, a few child participants mentioned that they would like to see their pictures for more time when they click/hover on their picture password. We also noticed the importance of proper education or training for children before they interact with the KidsPic authentication mechanism. The outcome of this research objective is a design and it's implementation of a mechanism (Figure 6.11) that mitigate the shoulder surfing attack on KidsPic authentication mechanism.

Table 6.5: The random probability guessing with respect to number of pictures in each category and total number of picture categories

# of categories / Number of pictures in each category	3	4	5	6	7	8	9
49	8.50×10^{-06}	1.73×10^{-07}	3.54×10^{-09}	7.22×10^{-11}	1.47×10^{-12}	3.01×10^{-14}	6.14×10^{-16}
64	3.81×10^{-06}	5.96×10^{-08}	9.31×10^{-10}	1.46×10^{-11}	2.27×10^{-13}	3.55×10^{-15}	5.55×10^{-17}
81	1.88×10^{-06}	2.32×10^{-08}	2.87×10^{-10}	3.54×10^{-12}	4.37×10^{-14}	5.40×10^{-16}	6.66×10^{-18}
100	1.00×10^{-06}	1.00×10^{-08}	1.00×10^{-10}	1.00×10^{-12}	1.00×10^{-14}	1.00×10^{-16}	1.00×10^{-18}
108	7.94×10^{-07}	7.35×10^{-09}	6.81×10^{-11}	6.30×10^{-13}	5.83×10^{-15}	5.40×10^{-17}	5.00×10^{-19}
147	3.15×10^{-07}	2.14×10^{-09}	1.46×10^{-11}	09.91×10^{-14}	6.74×10^{-16}	4.59×10^{-18}	3.12×10^{-20}

6.8 RO7: Avoiding Guessing Attacks on KidsPic$_{108|7}$

6.8.1 Overview

Though it takes a long time to crack a password using a random guessability attack (see Table 6.5) — it is relatively easy to crack a password using a guessing attack by knowing little about the user. A "Guessing attack" is one of the known possible attacks for any authentication system. In relation to the graphical authentication mechanism KidsPic, one might wonder whether someone close to a particular user

might be able to guess that user's picture password. As such, it could be possible for people who live in the same household to know enough about another member of the household to be able to guess their password.

6.8.2 Participants Recruitment

Following the approved IRB protocol, I recruited a total of 13 child-dyads (n = 28) ages 6-11 via social media apps.

6.8.3 Methods and Study Procedure

From the data collected so far, children have chosen their pictures for the KidsPic authentication mechanism completely based on their own personal sentiments and attachments around those pictures (like their likes, or someone they know like an aunt likes that picture e.g. a child participant from Kidsteam mentioned that "I choose wonder women because my aunt who visited my home likes her."). One potential thing to explore is whether someone such as a sibling could easily guess their sibling's password, as they are likely to know their sibling's likes and dislikes. To evaluate this hypothesis, I conducted a study by recruiting child participants (13 child sibling pairs, ages 6-11). As part of this study, I submitted the protocol details to the IRB and received IRB's approval before I started recruiting child participants. This protocol is a single session protocol; after obtaining consent and assent forms from child participants, child siblings used KidsPic to create a username and password one at a time. After creating a username and password, they guessed their siblings password, and answered a few sets of open-ended questions about their password

choices and their guess about their sibling's password. Child-created usernames and passwords were stored in a central database. All the semi-structured interviews were audio recorded to not miss any details. I further transcribed and analyzed child participants' responses to the open-ended questions.

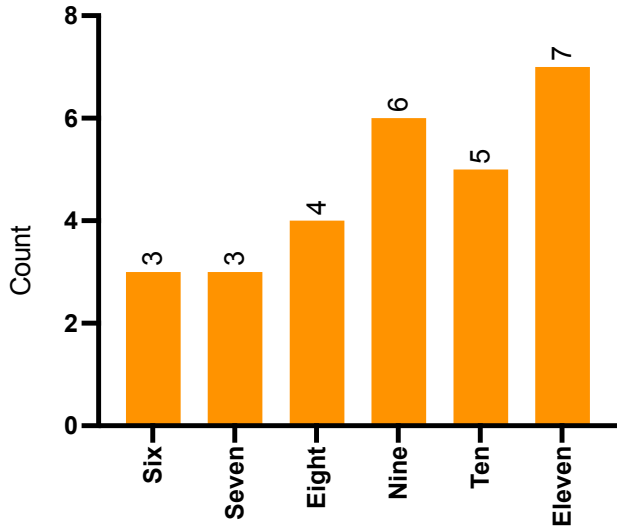


Figure 6.12: Age distribution of child participants participated in Research Objective 7.

6.8.4 Results and Analysis

We recruited 13 child dyads in this study. All the child participants are in the age range of 6-11, and the age distribution of child participants is depicted in Figure 6.12. We observed multiple child participants selecting the same picture for their created passwords; we observed the same behaviour in the Chapter 5 results. In other words, there was a duplicate selection of pictures in each picture category, and Figure 6.13 depicts the count of duplicate pictures in each picture category. We were also interested in seeing a significant difference between duplicate picture selection

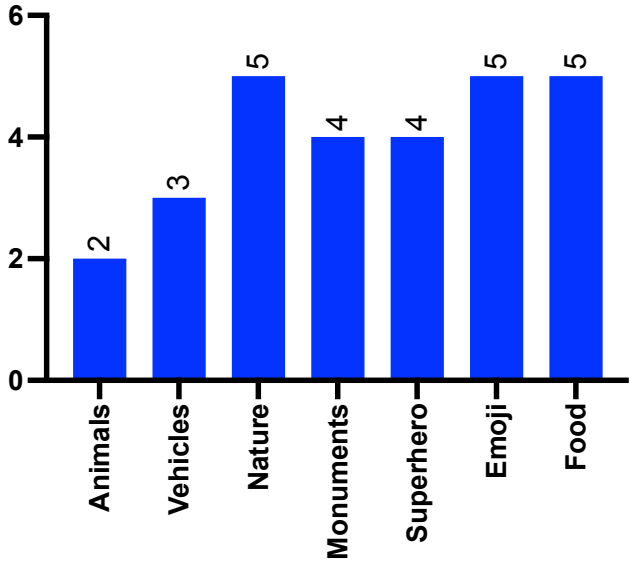


Figure 6.13: Duplicate pictures selected by child participants across picture categories.

between picture categories, and we did not observe any significant difference between picture categories.

Each child participant guessed three probable pictures in each category that their siblings might have chosen for their KidsPic password. This resulted in a total of 651 child participant guesses across the seven picture categories. Among the 651 guesses, child participants correctly guessed 15 pictures about their siblings' picture selection for their passwords. We were also interested to know the count of guesses in each of the attempts among three; there were six, three, one correct guesses in the first, second, and third attempts. There were 26 contextual guesses among 651 total guesses. The contextual guesses were when children could guess their sibling's passwords such as *"He definitely would've chosen a cat!"* but their siblings may have chosen a different cat picture. In the future, we should encourage children to not

choose password pictures that are closely associated with their sentiments.

CHAPTER 7

CONCLUSION AND FUTURE DIRECTIONS

The increase in usage of technologies requires people to create and use profiles for the apps and online services they use in day-to-day life. The apps and online services store users' personally identifiable information (PII) associated with their profiles. PII is valuable and considered very sensitive information in this digitally advancing world. Though there are robust regulations that exist across the globe to handle PII, there are many instances of data breaches that have occurred targeting users' PII. Creating a strong username and password is one way that will help users securely save their PII in apps or online services they use. As technology increases, users must create more online accounts, and this behavior is not limited to adults. Based on the literature, children are not an exception in using technology in their day-to-day life. They use technology and create online accounts starting from playing online games to apps at school. Existing literature suggests that children suffer from memorability issues while using online applications, which require them to create and remember usernames and passwords. This dissertation presents the design, development, and evaluation of web-based graphical authentication mechanism *KidsPic*, which reduced memorability issues for children. In this chapter we present a summary of findings of the research objectives addressed and the future direction of this work. The summary

of research objectives solved, and our contributions through this dissertation are as follows:

7.1 Understanding Children Authentication Practices

As a first step in designing and developing an authentication mechanism for children, we investigated children's authentication practices and adults' (parents and teachers) involvement in creating and using passwords by children. We conducted semi-structured interviews with children (n=22, ages 6-11) and a survey questionnaire with adult participants (n=33, 25 parents, 5 teachers, 3 both parents and teacher). We utilized alphanumeric, pattern, and numeric password mechanisms to understand children's authentication practices. Children created usernames and passwords using above-mentioned authentication mechanism and answered a few sets of open-ended questions. Most of the child participants created self-related usernames and passwords or re-used their credentials from their existing ones.

From the observations of collected results, it is clear that children are suffering from memorability issues in remembering their created usernames and passwords. To avoid memorability issues, they adopt weak authentication practices like writing their credentials on paper, reusing them from other accounts, creating self-related credentials, and using their parents' help to remember their credentials. Thirty-one adult participants completed the survey. The survey responses indicated that adults help their children create and use usernames and passwords because of their children's memorability issues. We utilized the SEBIS scale to gauge adult respondents' online security behavior. The analysis of adult survey responses, particularly the SEBIS

scale, revealed there is a gap in theoretical and actual behavior with regards to usernames and passwords creation and re-use. In this study, we observed that children suffer from memorability issues in using existing authentication mechanisms. The analysis of the findings is a clear indication that there is a need to develop an authentication mechanism for children that is usable by reducing their memorability issues and that still provides security.

7.2 Graphical User Authentication Mechanism (KidsPic) for Children

From the literature, it is clear that humans can remember pictures better than the text. As such, I designed and developed a graphical-based authentication mechanism called $KidsPic_{16|4}$. The $\text{KidsPic}_{16|4}$ has 16 pictures on each screen, and in total, there are four screens. The pictures used in this mechanism are kid-friendly. Children choose one picture from each screen, and a total of four pictures comprises their password. To evaluate the usability of $\text{KidsPic}_{16|4}$, we conducted four formative studies with Kidsteam. Each formative study is exactly one week apart. In the formative studies, we asked children to create passwords using $\text{KidsPic}_{16|4}$, an alphanumeric authentication mechanism with and without password restrictions. We compared child participants' failed number of login attempts with respect to both alphanumeric and $\text{KidsPic}_{16|4}$ authentication mechanisms. Though there is no significant difference in the failed number of login attempts between alphanumeric and $\text{KidsPic}_{16|4}$ authentication mechanisms, we observed a relatively fewer number of failed login attempts with $\text{KidsPic}_{16|4}$ authentication mechanism. The fewer number of failed

login attempts with KidsPic$_{16|4}$ authentication indicates that children were able to remember their created password with KidsPic$_{16|4}$ better than the alphanumeric authentication mechanism.

7.3 Enhancing KidsPic Usability and Theoretical Password Space

From the formative studies, we observed fewer failed login attempts with KidsPic compared to the alphanumeric authentication mechanism. Children could remember their passwords better using KidsPic, which indicates that KidsPic is usable. It is essential to be both usable and secure as a good authentication mechanism. Using participatory design sessions with Kidsteam, we increased both usability and security of KidsPic. We conducted a large-scale usability study with KidsPic by recruiting children (n = 40, ages 6-11). This usability study had two sessions, and they were a week apart. In session one, children created passwords using both KidsPic and alphanumeric authentication mechanisms. Children entered their passwords after 15 minutes of a distraction task (in session one) and after a week (in session two). Both successful and failed login attempts were registered in the centralized database. During the analysis of collected data, we observed significantly fewer failed login attempts with KidsPic compared to the alphanumeric authentication mechanism after 15 minutes and a week. The results and analysis indicated that children were significantly better at remembering KidsPic password compared to an alphanumeric password.

7.4 Investigating Additional Aspects of Graphical Authentication

Though the enhanced version of KidsPic increased both usability and security, we noticed there were a few instances where multiple children chose the same picture, resulting in a duplicate selection of pictures. The duplicate selection resulted in children not utilizing the complete password space in KidsPic. We further investigated the reasons behind children not utilizing the complete password space by formulating some usability research objectives. The different usability research objectives included: **RO1:** Does a picture's resolution influence children to select a picture for their password? – **RO2:** Does a change in the order of picture categories reduce duplicate pictures? – **RO3:** Does the number of objects in each picture influence children to choose a picture for their password? – **RO4:** Do picture features, like dominant colors of pictures, influence children to choose a picture? We conducted a few usability studies and participatory design sessions to address these usability research objectives, and from the results, we found that children choose pictures purely based on their sentiments about the picture. From the obtained results in Chapter 4, 5 we learned that, KidsPic is prone to security attacks like brute force, shoulder surfing, and guessing attacks. We conducted participatory design sessions with Kidsteam to design a mechanism to mitigate brute force (**RO5**) and shoulder surfing (**RO6**) attacks. We recruited 14 child dyads and conducted semi-structured interviews to evaluate the guessability attack (**RO7**), and we found a few instances where child siblings guessed their brother/sister's exact picture choices. We observed successful password guesses as children chose pictures based on their sentiments (their

likes); in the future, we plan to ask children not to choose pictures based on their sentiments.

Future Directions

This research helped us learn several insights about picture passwords; however, more exploration of this research is possible, and I will explain the several possibilities of future work in this following section.

It is clear from this dissertation work that KidsPic significantly increased children's memorability in remembering their passwords. The critical elements that improved children's password memorability using KidsPic were graphical-based and story-making for selected pictures. In the future, it will be good to investigate and find out if a change in picture categories would further improve children's memorability and reduce the chances of children selecting duplicate pictures.

One analogy from the results, obtained from Chapter 3, is that children might choose the pictures for their passwords, which are familiar to them. For example, they may choose a cat picture as an animal picture for their password instead of choosing a "hippopotamus" that they do not see in their daily routine. In the future, it will be interesting to see if an increase/decrease in the number of familiar pictures will increase memorability and reduce the chances of children selecting duplicate pictures.

As technology usage increases, children use computers and mobile devices for their day-to-day activities. Because of the nature of the KidsPic, which displays 108 pictures per category, KidsPic is ideal for laptop or desktop screens. In the future, I

recommend that researchers should explore alternative ways to make KidsPic more adaptable for mobile devices like tablets.

The results from Chapter 5 indicate that child participants took a significant amount of time to create a password using KidsPic compared to the alphanumeric authentication mechanism. This is to be expected as children have to go through 108 picture options in each picture category and choose their picture password from each category. By doing so, KidsPic's theoretical password space increased; on the other hand, it takes time for children to make their passwords. While the time children take to create passwords helps them remember the password, it will be interesting to explore ways to reduce the password creation time by ensuring the memorability of KidsPic.

From Chapter 6, it is clear that children chose their passwords based on their sentiments around those pictures. In addition, it will be a good attempt to consider understanding children's cultural backgrounds and draw any correlations between their culture and their choice of pictures for the KidsPic password. For example, children from the United States of America may choose the Statue of Liberty from the monuments picture category. On the other hand, children from India may choose the Taj Mahal for their monument's picture category.

REFERENCES

[1] S. Egelman and E. Peer, "Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS)," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ser. CHI '15. New York, NY, USA: ACM, 2015, pp. 2873–2882, event-place: Seoul, Republic of Korea. [Online]. Available: http://doi.acm.org/10.1145/2702123.2702249

[2] M. B. Ben Brody. (2019) MS Windows NT kernel description. [Online]. Available: https://www.bloomberg.com/news/articles/2019-09-04/google-to-pay-170-million-for-youtube-child-privacy-breaches

[3] Verizon, "Data breach investigation report," 2020. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/

[4] "Nist digital identity guidelines," 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-63b

[5] S. Maqsood, S. Chiasson, and A. Girouard, "Bend Passwords: Using Gestures to Authenticate on Flexible Devices," *Personal Ubiquitous Comput.*, vol. 20, no. 4, pp. 573–600, Aug. 2016. [Online]. Available: http://dx.doi.org/10.1007/s00779-016-0928-6

[6] D. k. Ratakonda, T. French, and J. A. Fails, "My name is my password: Understanding children's authentication practices," in *Proceedings of the 18th ACM International Conference on Interaction Design and Children*, ser. IDC '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 501–507. [Online]. Available: https://doi.org/10.1145/3311927.3325327

[7] D. R. Lamichhane and J. C. Read, "Investigating Children's Passwords Using a Game-based Survey," in *Proceedings of the 2017 Conference on Interaction Design and Children*, ser. IDC '17. New York, NY, USA: ACM, 2017, pp. 617–622, event-place: Stanford, California, USA. [Online]. Available: http://doi.acm.org/10.1145/3078072.3084333

[8] J. C. Read and B. Cassidy, "Designing Textual Password Systems for Children," in *Proceedings of the 11th International Conference on Interaction*

Design and Children, ser. IDC '12. New York, NY, USA: ACM, 2012, pp. 200–203, event-place: Bremen, Germany. [Online]. Available: http://doi.acm.org/10.1145/2307096.2307125

[9] J. C. Read and 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*, ser. BCS-HCI '09. Swinton, UK, UK: British Computer Society, 2009, pp. 288–292, event-place: Cambridge, United Kingdom. [Online]. Available: http://dl.acm.org/citation.cfm?id=1671011.1671046

[10] J. Cole, G. Walsh, and Z. Pease, "Click to Enter: Comparing Graphical and Textual Passwords for Children," in *Proceedings of the 2017 Conference on Interaction Design and Children*, ser. IDC '17. New York, NY, USA: ACM, 2017, pp. 472–477, event-place: Stanford, California, USA. [Online]. Available: http://doi.acm.org/10.1145/3078072.3084311

[11] E. A. Kirkpatrick, "An experimental study of memory." psychological review," 1894.

[12] D. P. T. Tullis, Thomas S. and K. E. McCaffrey, "Can users remember their pictorial passwords six years later." 2011. [Online]. Available: https://doi.org/10.1145/1979742.1979945.

[13] D. Norman, ""the design of everyday things"," https://www.nixdell.com/classes/HCI-and-Design-Spring-2017/The-Design-of-Everyday-Things-Revised-and-Expanded-Edition.pdf., 2013.

[14] R. N.Shepard, ""recognition Memory for Words, Sentences, and Pictures."," ser. Journal of Verbal Learning and Verbal Behavior 6, no. 1 (1967): 156–63., 1967. [Online]. Available: https://doi.org/10.1016/S0022-5371(67)80067-7.

[15] "Accurate visual memory for previously attended objects in natural scenes.-psycnet." 2002. [Online]. Available: https://doi.org/10.1037/0096-1523.28.1.113.

[16] A. Druin, "Cooperative inquiry: Developing new technologies for children with children," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '99. New York, NY, USA: Association for Computing Machinery, 1999, p. 592–599. [Online]. Available: https://doi.org/10.1145/302979.303166

[17] M. L. Guha, A. Druin, and J. A. Fails, "Cooperative inquiry revisited: Reflections of the past and guidelines for the future of intergenerational co-design," 2012.

[18] B. Lorenz, K. Kikkas, and A. Klooster, ""the four most-used passwords are love, sex, secret, and god": Password security and training in different user groups," 07 2013, pp. 276–283.

[19] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13*, ser. SSYM'04. USA: USENIX Association, 2004, p. 11.

[20] M. D. Hafiz, A. H. Abdullah, N. Ithnin, and H. K. Mammi, "Towards identifying usability and security features of graphical password in knowledge based authentication technique," in *2008 Second Asia International Conference on Modelling Simulation (AMS)*, 2008, pp. 396–403.

[21] S. Garfinkel and H. R. Lipford, "Usable security: History, themes, and challenges. trust 5, no. 2 (2014): 1–124," 2014. [Online]. Available: https://doi.org/10.2200/S00594ED1V01Y201408SPT011

[22] S. Gaw and E. W. Felten, "Password Management Strategies for Online Accounts," in *Proceedings of the Second Symposium on Usable Privacy and Security*, ser. SOUPS '06. New York, NY, USA: ACM, 2006, pp. 44–55, event-place: Pittsburgh, Pennsylvania, USA. [Online]. Available: http://doi.acm.org/10.1145/1143120.1143127

[23] P. Kumar, S. M. Naik, U. R. Devkar, M. Chetty, T. L. Clegg, and J. Vitak, "'No Telling Passcodes Out Because They'Re Private': Understanding Children's Mental Models of Privacy and Security Online," *Proc. ACM Hum.-Comput. Interact.*, vol. 1, no. CSCW, pp. 64:1–64:21, Dec. 2017. [Online]. Available: http://doi.acm.org/10.1145/3134699

[24] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password memorability and security: Empirical results." *Security Privacy, IEEE*, vol. 2, pp. 25 – 31, 10 2004.

[25] S. Maqsood, R. Biddle, S. Maqsood, and S. Chiasson, "An exploratory study of children's online password behaviours," in *Proceedings of the 17th ACM Conference on Interaction Design and Children*, ser. IDC '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 539–544. [Online]. Available: https://doi.org/10.1145/3202185.3210772

[26] S. Brostoff and M. A. Sasse, "Are passfaces more usable than passwords? a field trial investigation," in *People and Computers XIV — Usability or Else!*, S. McDonald, Y. Waern, and G. Cockton, Eds. London: Springer London, 2000, pp. 405–424.

[27] M. G. Tuscano, "Graphical password authentication using Pass faces," 2015. [Online]. Available: https://www.ijera.com/papers/Vol5_issue3/Part%20-%205/M503056064.pdf

[28] P. Dunphy, J. Nicholson, and P. Olivier, "Securing Passfaces for Description," in *Proceedings of the 4th Symposium on Usable Privacy and Security*, ser. SOUPS '08. New York, NY, USA: ACM, 2008, pp. 24–35, event-place: Pittsburgh, Pennsylvania, USA. [Online]. Available: http://doi.acm.org/10.1145/1408664.1408668

[29] M. Hlywa, R. Biddle, and A. S. Patrick, "Facing the facts about image type in recognition-based graphical passwords," in *Proceedings of the 27th Annual Computer Security Applications Conference*, ser. ACSAC '11. New York, NY, USA: Association for Computing Machinery, 2011, p. 149–158. [Online]. Available: https://doi.org/10.1145/2076732.2076754

[30] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13*, ser. SSYM'04. USA: USENIX Association, 2004, p. 11.

[31] R. V. Yampolskiy, "Analyzing user password selection behavior for reduction of password space," in *Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology*, 2006, pp. 109–115.

[32] A. Bhanushali, B. Mange, H. Vyas, H. Bhanushali, and P. Bhogle, "Article: Comparison of graphical password authentication techniques," *International Journal of Computer Applications*, vol. 116, no. 1, pp. 11–14, April 2015, full text available.

[33] J. Thorpe, M. Al-Badawi, B. MacRae, and A. Salehi-Abari, "The Presentation Effect on Graphical Passwords," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '14. New York, NY, USA: ACM, 2014, pp. 2947–2950, event-place: Toronto, Ontario, Canada. [Online]. Available: http://doi.acm.org/10.1145/2556288.2557212

[34] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in *8th USENIX Security Symposium (USENIX Security 99)*. Washington, D.C.: USENIX Association, Aug. 1999. [Online]. Available: https://www.usenix.org/conference/8th-usenix-security-symposium/design-and-analysis-graphical-passwords

[35] H. Gao, X. Guo, X. Chen, L. Wang, and X. Liu, "Yagp: Yet another graphical password strategy," in *2008 Annual Computer Security Applications Conference (ACSAC)*, 2008, pp. 121–129.

[36] A. De Luca, R. Weiss, and H. Drewes, "Evaluation of eye-gaze interaction methods for security enhanced pin-entry," in *Proceedings of the 19th Australasian Conference on Computer-Human Interaction: Entertaining User Interfaces*, ser. OZCHI '07. New York, NY, USA: ACM, 2007, pp. 199–202. [Online]. Available: http://doi.acm.org/10.1145/1324892.1324932

[37] A. Forget, S. Chiasson, and R. Biddle, "Shoulder-surfing Resistance with Eye-gaze Entry in Cued-recall Graphical Passwords," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '10. New York, NY, USA: ACM, 2010, pp. 1107–1110, event-place: Atlanta, Georgia, USA. [Online]. Available: http://doi.acm.org/10.1145/1753326.1753491

[38] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle, "Multiple Password Interference in Text Passwords and Click-based Graphical Passwords," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 500–511, event-place: Chicago, Illinois, USA. [Online]. Available: http://doi.acm.org/10.1145/1653662.1653722

[39] H.-M. Sun, Y.-H. Chen, C.-C. Fang, and S.-Y. Chang, "PassMap: A Map Based Graphical-password Authentication System," in *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, ser. ASIACCS '12. New York, NY, USA: ACM, 2012, pp. 99–100, event-place: Seoul, Korea. [Online]. Available: http://doi.acm.org/10.1145/2414456.2414513

[40] T. Takada, T. Onuki, and H. Koike, "Awase-e: Recognition-based image authentication scheme using users' personal photographs," in *2006 Innovations in Information Technology*, Nov 2006, pp. 1–5.

[41] J. W. Creswell, *Qualitative inquiry and research design: choosing among five traditions*. Sage Publications, 1998, google-Books-ID: bjO2AAAAIAAJ.

[42] K. Charmaz and L. L. Belgrave, "Qualitative interviewing and grounded theory analysis," *The SAGE Handbook of Interview Research: The Complexity of the Craft*, pp. 347–366, Jan. 2012. [Online]. Available: https://miami.pure.elsevier.com/en/publications/qualitative-interviewing-and-grounded-theory-analysis

[43] L. Zhang-Kennedy, C. Mekhail, Y. Abdelaziz, and S. Chiasson, "From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats," in *Proceedings of the The 15th International Conference on Interaction Design and Children*, ser. IDC '16. New York, NY, USA: ACM, 2016, pp. 388–399, event-place: Manchester, United Kingdom. [Online]. Available: http://doi.acm.org/10.1145/2930674.2930716

[44] ""text worlds," in cognitive poetics: Goals, gains, and gaps," 2009.

[45] C. E. Shannon, "Prediction and entropy of printed english," *Bell System Technical Journal*, vol. 30, no. 1, pp. 50–64, 1951. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/j.1538-7305.1951.tb01366.x

[46] M. Hlywa, R. Biddle, and A. S. Patrick, "Facing the facts about image type in recognition-based graphical passwords," in *Proceedings of the 27th Annual Computer Security Applications Conference*, ser. ACSAC '11. New York, NY, USA: Association for Computing Machinery, 2011, p. 149–158. [Online]. Available: https://doi.org/10.1145/2076732.2076754