A COMPARISON OF PASSWORD AUTHENTICATION BETWEEN CHILDREN AND ADULTS

by
Ahsan Imran

A thesis submitted to
the Faculty of Graduate and Postdoctoral Affairs
in partial fulfillment of
the requirements for the degree of

MASTER OF SCIENCE

School of Computer Science

at

CARLETON UNIVERSITY

Ottawa, Ontario
September 2015

Abstract

According to a large MediaSmarts survey, 99 percent of Canadian children aged 8-15 are online. We already have a good number of security measures for adults but can those measures keep children secure as well? As a starting point, we explore the subject of user authentication for children.

We conducted two studies on three graphical password schemes (Objects, Image and Words PassTiles), one with adults and one with children. We analyse the data collected from these 50 participants to compare their performance and preferences. Although outperformed by the adults, children performed best with Objects PassTiles where they recognized images of distinct objects from among decoys. Adults and children both have similar opinions, including a preference for graphical passwords over their existing password schemes. We conclude the thesis with four recommendations based on our experiences.

Acknowledgements

Firstly, I would like to express my sincere gratitude to my supervisor Sonia Chiasson for her continuous support, guidance and enthusiasm without which this thesis would not have been possible. Thank you for all the wisdom and knowledge that you have shared with me throughout the research.

My sincere thanks also goes to Robert Biddle for his technical guidance in setting up the system on which the studies were conducted. Thank you very much for your expertise.

I thank the members of my committee, Robert Biddle and Timothy Lethbridge for their time, feedback and insightful comments. I would also like to thank Oliver van Kaick for chairing the meeting of my thesis defence.

Lastly, I would like to thank my parents and sisters for all their love, motivation and encouragement throughout the writing of this thesis.

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

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Motivation

Adults are not the only ones in need of online security and privacy. The number of children who have access to the Internet is increasing rapidly. According to a 2014 survey, 99 percent of Canadian children aged 8 to 15 years use the Internet [44]. The statistics are similar in other areas of the world, such as the UK [43] and Australia [7]. This increased access leads to increased worry, for example, 36 percent of US parents with children over 5 have had concerns over their children's Internet use in the last year [28]. Since children now constitute a significant portion of people who use the Internet, we need to consider new ways of keeping both adults and children secure from online attacks. Children and adults do not necessarily have the same skills and preferences and children may benefit from a different authentication system designed specifically to better suit their needs.

Although some products exist to generate "child-friendly" text passwords [42], little research has been conducted on authentication systems for children. The main focus of online security for children has been on designing methods that adults can use to protect children [15] [9], such as parental controls limiting access to online resources or tools to monitor children's online behaviour. Of the work aimed at children, most attempt to teach them of the dangers of Internet usage [37] rather than designing authentication methods or mechanisms that children would find easier to use themselves, without the help of an adult. Therefore, through this study we seek to address this gap by exploring the usability of graphical passwords for children, which could ultimately lead to the developments of authentication mechanisms different from existing adult password schemes, and more adaptable to the needs of children.

1.2 Research Question

The main research question for this thesis is:

How does children's performance and opinion of graphical passwords compare to that of adults?

We find the answer to this question by conducting user studies with both adults and children which require them to interact with three graphical password schemes: Objects PassTiles, Image PassTiles and Words PassTiles. We explore the similarities and differences in the performance of adults and children during password creation, first login, and second login, as well as ask their personal preferences from among the three PassTile variants. We compare the results to determine the answer to this research question.

1.3 Contribution

This thesis has two main contributions resulting from the research. These are summarized in the following sections.

1.3.1 A comparison of user authentication for children and adults

We conduct two user studies, one with adults and the other with children, in which we evaluate their performance with three password schemes. We provide empirical results from 50 participants evaluating both performance and perception data. We found that both adults and children prefer graphical passwords to their existing ones. Children performed best with Objects PassTiles scheme, where they had to recognize five distinct objects among decoys. Adults outperformed children in the Objects PassTiles scheme by having significantly higher success rates whereas their success rates for Image and Words PassTiles were similar. Both adults and children had similar opinions of the schemes.

1.3.2 Recommendations on adapting user authentication for children

Based on our experiences, we offer four recommendations. Two of these apply to both children and adults, while two are targeted at authentication for children specifically.

Objects PassTiles should be made available for low-to-medium security accounts as it had the best performance from both adults and children from among the three password schemes. We would also recommend facilitating memorization for children through learning and training features by linking the words or objects together to form stories. We would recommend adapting an interface which is age-appropriate for children by incorporating familiar objects and words as well as using an easy input method. We recommend combining schemes to improve memorability like using words with pictures to provide additional cues that could help with memorization.

1.4 Thesis Outline

This thesis consists of six chapters. In the second chapter, we provide some background research done on graphical passwords, authentication for adults and children and previous user studies done with children in the field of human computer interaction. In the third chapter, we explain the system that we used to conduct the user studies. We also give an overview of the three PassTile variants used in the studies along with the modifications made to the interface. In the fourth chapter, we describe the methodology for the user studies conducted with adults and children. In the fifth chapter, we outline our hypotheses and analyse the data collected from the participants' performance and interviews. This data includes login success rates, degree of correctness, login times, memorization times and preferences. We look at the results to see whether they support our hypotheses. Finally in chapter six, we present a discussion of the results and our observations from the studies. We also present the conclusion to our thesis.

Chapter 2

Background

Before looking at the study involving the comparison of adult and child password authentication, we review some prior work done within the context of this research. This includes authentication, password security for children and adults, graphical passwords, children's user studies and human computer interaction for children.

2.1 Authentication

Authentication is the process of determining whether someone is, in fact, who they declared themselves to be. There are three common ways to authenticate an individual in computer systems. It can be through something the person knows, like passwords, by something the person has, like a physical key card, or by something the person is or does (Biometrics) [39] [8]. Hamilton et al. [24] examine various authentication methods and mechanisms available today, and determine which is appropriate for various uses. They discuss the advantages and disadvantages of several authentication mechanisms, including Smartcards, biometrics, centralized authentication, behaviour based authentication and authentication recovery.

The most common types of authentication are knowledge-based, meaning that the user must remember the shared secret. The strongest passwords are randomly generated, but often users instead choose passwords with meaningful content. A non-meaningful item can be learned effectively if the person puts effort into learning it, but it will frequently decay within 30 days [20]. However, the item can be made meaningful by linking it to a previously learned item such as a birthday. There are three ways an item can be remembered: uncued recall, cued recall and recognition [16]. For uncued recall the person has to extract the item from memory without any outside cues. This is usually the case with text passwords and PINs. For cued recall, a person is given a cue and uses it to extract the item from memory. For recognition, a person

is shown the item and then has to confirm whether this is the previously encoded item. We study two recognition based graphical passwords (Objects and Words PassTiles) and one cued recall graphical password (Image PassTiles) within our research.

The most popular authentication mechanism is the uncued recall passwords which ideally consist of a random sequence of characters. There is evidence that users remember these passwords better if they choose them [58], even though system-assigned passwords tend to be stronger. Many users become overloaded with too many passwords to remember and hence do not choose strong passwords. Spector et al. [41] determine whether users remember the semantics of a passphrase for authentication instead of relying only on the syntax as is the case with usual passwords. Passphrases are a good alternative to passwords as they address both memorability and predictability issues.

On the Internet, the use of passwords is the primary means of authenticating a user. There are different types of passwords available to authenticate users online. These include alphanumeric, PINs and graphical passwords. The context of our study is on graphical passwords for both adults and children.

2.1.1 Children

First we look at the existing research on authentication for children. There is not a lot of existing research in this field as the focus has primarily been on adults and how we could make improvements in password authentication that would benefit adults. We summarize the sparse literature on authentication for children.

Read et al. [35] did two user studies on passwords for children. The first examined children's knowledge and creation of text based passwords and the second investigated the passwords that children chose to use. Children have an understanding of how to make a good textual password but those passwords they use are often not according to their own knowledge of best practice. The participants were between the ages of 6 and 10. Younger and older children appeared to have equally simple passwords made solely out of words some of which were misspelt. On the positive side, the passwords could not be easily derived from the username. It is suggested that password length for children should be between four to eight characters and associated with a secondary

question-based prompt to increase security.

Mendori et al. [29] describe a new password input interface using icons for primary school children. They argue that alphanumeric passwords appear too difficult for children who have not yet learned the Roman alphabet. A study was conducted with a password interface which used icons familiar to primary school children. This system was evaluated with different parameters such as the number of icons, icon selection time and frequency of use. The categories of icons included fruits, colours, animals and flowers. Results showed that although the components of a password could be memorized, children made mistakes in the input order.

Collela et al. [15] filed a patent that would allow secure Internet access for children. This security system is based on a card reader which is assigned to each child along with a card containing an integrated biometric fingerprint scanner. Each child registers their card with a unique ID and under authorization of their parents who can apply parental control settings to the system. The child can access the Internet through any web enabled computer by plugging in the card reader to the computer, inserting their security card and then scanning the fingerprint. This would give them restricted access to the Internet under the parental control settings selected by their parents. To date, this system has not been made publicly available.

Another patent developed by Tse et al. [53] presents a game-like multi-level authentication mechanism geared towards younger users. Multiple verification attributes are collected throughout the interaction between the user and the device which means that user goes through several authentication mechanisms. When the user reaches a certain level of identification they are then marked as authenticated. This procedure, although longer than the usual way of authentication through typing text passwords, reduces the user's memory load. It also provides an environment that is fun for young users and requires little training. A user would be provided with challenges and, as he completes each one, the data is stored for comparison the next time he attempts the same challenge. We found no publicly available implementation of this scheme.

Channakeshava et al. [9] provided a privacy enhancing framework called POCKET (Parental Online Consent for Kids' Electronic Transaction). Parents answer a few

privacy related questions and POCKET automatically converts them to a privacy preference file which restricts the child's Internet access according to these preferences. POCKET provides a simple interface for parents to configure privacy choices for their child, and then automatically enforces these policies. It is implemented as a prototype intended for technologically unsophisticated parents to protect their child's privacy. Parents can control the personal information collected by websites from the child without constantly monitoring their activities online. This tool was tested through focus groups where parents were asked to participate in a study using POCKET and asked about how they protect their children's privacy. It was found that the ways parents use to control what children view online include placing computers in plain view or telling children they could track sites browsed (even though the parents did not know how).

Ervasti et al. [21] conducted a security based trial using Near Field Communication Technology (NFC) at a primary school where pupils between ages of 6 and 8 marked their arrival at and departure from school by touching their smart card with a smart card reader device. It also allows parents to follow in real time their children's attendance status in school. The teachers could gather information about children's attendance and keep logs about their possible lateness at school. User research revealed that for the children of this age, as well as for their parents, the concept of being monitored by this technology is something that they welcome. This system was an easy authentication mechanism for children of early age who are in the stages of learning to read and write.

2.1.2 Adults

There are several existing research projects on different methods of authentication for adults. These include image based authentication as well as biometric authentication for mobile devices. We highlight a few relevant papers.

Takada et al. [51] introduce a new method of authentication for mobile phones called 'Awase-E'. This system is based on using image authentication, which is more user-friendly than passwords or 4-digit PINs. A longer password offers more protection but at the same time it takes a longer time to input and is thus undesirable.

This method is used for phones with a digital camera. The images taken by the user from this camera are used instead of passwords. The user can add his or her favourite images to the authentication system. When a photo is registered, Awase-E sends an email to the user containing a URL with the web page, which has the same photo that the user has registered. If somebody other than the user is trying to register a photo, the user will be alerted and hence he will become aware of the security breach. The selection of images can also contain a 'pass-image' where the user does not have to select anything. This form of authentication has a few advantages over passwords. It is easier to memorize an image than a text. The notification by Email gives users a trigger to take action against intrusions. Using image registration and notification interfaces it combines aspects of usability and security and there is less of a trade-off between the two. This research shows that authentication can be based on photo images taken in real time instead of having to enter a text password. This is an alternative way of using images for authentication as compared to using them in graphical passwords.

Burnett [8] argues that the more methods of authentication you use, the more secure and reliable the authentication becomes. Combined with passwords, other forms of authentication such as biometrics can enhance the reliability of passwords e.g. a thumbprint or a retinal scan. He talks about basing authentication on three elements: something you know, something you have or something you are. The methods can be most effective when used in a combination. Using one method is fallible but combining two or more can greatly increase security. Biometric systems are at time unreliable and can show false positives. Facial recognition for example, has been bypassed by simply holding up a picture of the target's face in front of the camera. In his book, Burnett focuses more on how to build strong passwords to provide high security, but also emphasizes the need to have multiple layers of security for maximum protection. Many systems now use two factor authentication. Graphical passwords could be used as one of the factors.

Stobert et al. [47] conducted interviews to investigate how users keep track of many accounts and passwords. They found that most users cope by reusing passwords and

writing them down. Users are told not to create weak passwords, not to reuse passwords on multiple accounts, and not to write their passwords down. They are often required to change their passwords at regular intervals. One possible solution to the password problem is password managers, which store and enter users' passwords, thus saving the user from remembering their passwords or which passwords are associated with which accounts. However, they also have potential drawbacks such as difficulties with portability and potential consequences if the password manager is compromised.

Alphanumeric passwords still remain the most common authentication mechanism but we need alternatives that might address these problems. Graphical passwords show some promise at fixing several of these issues.

2.2 HCI for children

Several advancements have been made in the field of Human Computer Interaction for children. Research has been done to understand how children think and behave while interacting with computers since it cannot be assumed that systems designed and tested with adults will automatically also apply for children.

Read et al. [34] conducted a study to gather insights into security requirements for children. This design activity, referred as Participatory Analogy, presents design solutions that emerged following analysis of the children's contributions. Children were asked to identify their special things and then examine how they would keep them safe. This study was carried out with pictures rather than written text and participants were 8 to 10 years of age. The goal of the study was to determine how children's products could be designed to ensure that children understood how to keep special digital content, for instance passwords and personal data, secure.

Jennifer A. Rode [37] describe a study of children and parents looking at issues of domestic privacy and security. It provides an overview of parental rules and strategies for keeping children safe and discusses children's perspective on their online safety. It also reflects on the problematic state of privacy and ethics review boards when working with children. A set of interviews were conducted with the parents and children and a field study was conducted in their homes to test security software. Results of the study show that children tend to put themselves at risk and are largely unconcerned

about security. Children's privacy is not taken into account in computer architectures. Young children cannot read technical language in pop-up messages which could lead to breaches in security. The authors conclude that security technologies must consider the larger socio-technical context of use. The paper also discusses how access to children as informants is restricted by ethical boards and that this must be resolved so that researchers can gain sufficient access to understand how children use these technologies, while respecting the children's privacy and time.

Bruckman et al. [6] explain children's development as a series of stages and recognize the need of different computer interfaces for children throughout development. Children from ages 7 to 11 have been classified as being on the concrete operational stage. In this stage, children are able to use relatively sophisticated software, control the mouse, group similar items and characterize, while also being able to appreciate a playful approach. Characteristics such as dexterity, speech, reading, background knowledge and interaction style have also been discussed as being relevant for HCI research. Children have problems with marquee selection (selecting multiple objects using a shape) as well as dragging and double-clicking. Moreover, children from the age 9 to 11, prefer a bigger font for words while reading and prefer simple, playful and spontaneous interactions with technology. Furthermore, the authors stress the fact that children develop differently due to cultural or social factors which complicates the development of a user interface for a diverse population of children.

Antle [1] explains the concept of Embodied Cognition and why it is important in designing children's interactive technologies. Embodiment refers to how the nature of person's cognition is shaped by the form of its physical manifestation in the world as well as the role the environment plays in the development of cognitive processes. Apart from existing technologies, interaction designers and researchers should think of new ways in which children can interact with computers. She suggests that while learning a new system interface the body may remember what the mind does not. When children learn a new system interface, their mind might not remember a specific task performed but they might be able to offload memory from a cognitive realm to a realm based on interactions between the body and the environment. Hence, applications that provide an interactive environment for children that support the

interplay of action, cognition and the environment might prove to be successful.

2.3 Children's User Studies

Children are increasingly online. Although not directly related to security, the following studies observe their behaviour and interactions in online scenarios. These studies follow a similar methodology to our own by recruiting children within a specified age range and either having them use a system or asking them questions to gain more insight about how children spend time online.

Several studies have compared children and adult behaviours in online activities and found differences between groups. For example, researchers have explored online searching strategies. Druin et al. [19] investigate the Internet searching process that children go through by conducting a home study on 83 children between the ages of 7-11 years. Children make up a significant portion of Internet users who want to seek information but are faced by certain barriers. Children have different abilities to formulate queries and also to comprehend search results as compared to adults. They face challenges in understanding what to type and what tools are available. In this study, roles such as age, gender and who influences the child's searching are investigated.

Previous studies have shown that children initiate searches due to lack of understanding of a particular topic [26] but this study showed that children initiate search sessions for various reasons including a desire for social interaction or searching recreationally. Children also differ from adults while selecting from the list of sources that come up, and might experience difficulty, as they prefer to have results that exactly match their queries. Taking into account the visual context of searching, some children preferred to search entirely within a visual context and were interested in graphics. Given children's difficulties with traditional text interfaces and preferences for visual interfaces, it seems plausible that they might also favour visual means of authentication such as graphical passwords.

Keeping in mind that children are a rapidly growing segment of Internet users, it is important to gain knowledge of the factors that influence their abilities to navigate websites and process information. Hence, in this study, Rose et al. [38] investigate the

influence of Web site design on the information processing performance of children. The results from the study indicate that the age of the child moderates the relationship between the design of the Web site and search and learning performance. Younger children from the ages of 7 to 9 were able to recall more content using a map than a list of content and also when learning cues were used. Older children from the ages of 10-12 performed equally from both a content list and map, and with or without any learning cues. The authors suggest that websites should be customized to the abilities of children of different ages and interface design characteristics such as navigational aids and learning cues should be employed to facilitate search accuracy and information recall. For younger children, websites that have a visual map to aid search should be designed so that they are more child friendly.

Cycowicz et al. [17] conducted an experiment in which they asked children of age 7-8 years and adults to remember pictures drawn in red or green for an item memory test. In another task, they were asked to remember both the pictures and their associated colors for a source memory test. Item memory is about the occurrence of an event and is based on the content, whereas source memory relies on the context in which knowledge about the event was acquired. New and old pictures were presented in black. In the recognition task, participants were asked to make old/new recognition judgements, while in the source task, they were asked to make old-green old-red/new source judgements. Performance on all tasks improved with increasing age, but the age difference for source was much larger than that for item memory. The authors suggest that the frontal lobes play a critical role in the retrieval of source information, therefore, it is possible that immaturity of the frontal lobes may be causally related to the children's lower performance on the source memory task.

Borges et al. [3] compared recall and recognition performance between adults and children using three modes of presentation (written words, black-and-white pictures of objects, and color pictures of objects). The results showed a developmental trend of increasing recall performance with age. Children have pictorial and color cues available in memory in a manner very similar to adults. For adults, the greater the number of feature cues describing each item (labels, pictorial cues, color cues), the

greater their ability to recall the item. For children, each new item that was presented had the same probability of being remembered, regardless of the feature cues that could have distinguished that item from the others. This suggests that graphical passwords designed for children should have simple pictures and not too much information associated in terms of labels or text because it would be meaningless.

In a survey conducted by Steeves [44] of children between grade 4 and 11, it was found that portable devices like laptops and tablets are used more by children as compared to desktop computers. The most frequent online activities reported by children are playing online games, downloading music, using social networking websites and using Twitter. Almost one-third of students in grades 4-6 have a Facebook account and 16 percent also have Twitter accounts. Some of the websites that are most commonly visited by children are YouTube, Facebook, Twitter, Google, Minecraft and Hotmail. We note that most of these websites require a user account and password for access, and that these are used despite the fact that several have age restrictions in place. The majority of the students are aware of the risks of talking to strangers online. Children are confident in their ability to protect themselves online, with 77 percent of Grade 4 students indicating this. Parental supervision is high among children of grades 4-6 but almost one-third never sit with an adult or parent when online.

2.4 Graphical Passwords

Graphical passwords have been around for a long time and several studies have been done to compare the usability and security of different types of graphical passwords against text based password [14] [25] [5] [55] [11]. In several cases, a graphical password might be easy to use and remember due to visual cues but might lack the security and privacy due to threats such as shoulder surfing. We look at several user studies done with different graphical passwords.

Cognitive studies have shown that humans have a vast memory for pictures [27]. Prior research has shown that visual memory does not seem to be significantly affected by the general decline of cognitive abilities associated with aging [32]. Therefore, graphical passwords which are associated with pictures and images might make a

much more memorable password as compared to text based passwords.

Biddle et al. [2] review the usability and security aspects of different types of graphical passwords. These include recall based graphical password schemes such as Draw-A-Secret [25] where users create their password by drawing it on a 2D grid and the log in by repeating the same path through the grid cells. As there are no visual cues, these passwords are completely recall based. Another category of graphical passwords is recognition based where users have to memorize certain images during password creation and then recognize those images from among decoys to log in. Passfaces [5] is an example of this type of scheme where users have to remember certain faces as their password. Deja Vu [33] also works through recognizing several images in repeated rounds of selection but uses abstract images and photographs rather than faces. Cued Recall graphical passwords require users to remember certain locations in an image as their password. These are easier to memorise as compared to pure recall passwords. PassPoints [55] has been given as an example of this type of password, where a user selects an 5 points in an image as their password and then logs in by clicking on those points in the same order.

Suo et al. [50] conducted a survey to determine the strengths and limitations of recognition based and recall based graphical passwords. Given current technologies, it is more difficult to break graphical passwords using attack methods like brute force search, dictionary attack, and spyware. In terms of usability, recognition based graphical passwords take a lot of time during the registration and log in process. During registration, a user has to pick images from a large set and during authentication, a user has to scan many images to identify a few pass-images. The major issue for recall-based graphical passwords, like Draw-A-Secret, is the reliability and accuracy of algorithms to process user input. Another issue is that graphical passwords require much more storage space than text based passwords because a large number of pictures would have to be maintained in the database.

Angeli et al. [18] present the design and evaluation of Visual Identification Protocol (VIP) which uses simple representative images to authenticate users based on recognition. These are compared with PIN passwords and it is revealed through the user study that visual passwords are easier to remember, preferred by users, and more

secure than the numeric passwords.

Renaud et al. [36] evaluate a graphical password based on a visuo-spatial mechanism in which a user id required to position a coloured template onto an image with a grid superimposed over it in order to reveal a password. Several problems were revealed during this study such as choosing the right background image which offers a wide range of memorable locations. Another problem relates to user difficulty in pinpointing a particular location on the screen. In conclusion, it is very difficult for visuo-spatially based schemes to make a good authentication mechanism.

We now take a closer look at previous research done on the cued recall graphical passwords similar to Image PassTiles and results obtained from the studies done with those passwords.

Wiendenbeck et al. [54] study the effects of image and tolerance in PassPoints. The results of the study show that accuracy is greatly reduced when using a small tolerance area around the user's password points. The results of the study also suggest that background images with high diversity may support memorability in graphical password systems. A user may choose images that make a memorable password but it may have hot spots that attract many users to select the same points in the image.

Chiasson et al. [12] discuss how patterns appear across different images in click based graphical passwords such as PassPoints. These patterns reduce the security of the password by motivating attacks which are independent of the background image. In Cued Click Points passwords [14], each image provides a cue for the corresponding click-point, therefore reducing the tendency towards forming a geometric pattern. Persuasive Cued Click Point passwords [11], try to persuade users to select more random points, making it much less convenient to select hotspots and hence providing better security.

Everitt et al. [22] present a study of multiple graphical passwords by examining the frequency with which a graphical password is accessed, interference resulting from simultaneous access to multiple graphical passwords, and patterns of access while training multiple graphical passwords. All of these factors significantly impact the ease of authenticating when using multiple graphical passwords. Participants who accessed four different graphical passwords per week were ten times more likely to

completely fail to authenticate than participants who accessed a single password once per week.

Tari et al. [52] examine the real and perceived vulnerability to shoulder-surfing of two configurations (Keyboard input and mouse input) of the graphical password Passfaces, compared to non-dictionary and dictionary passwords. Input mechanisms for data entry (i.e., mouse versus numeric keypad) is an important consideration for graphical passwords like Passfaces. Dictionary passwords are less vulnerable to shoulder-surfing than non-dictionary passwords and Passfaces with mouse. Passfaces with keyboard entry was the least vulnerable to shoulder-surfing.

2.5 Summary

Based on the literature, there is a clear gap in user authentication for children. There is almost no existing research on children's use of passwords yet children have an increasing number of user accounts. Several characteristics of children point to better performance with images so graphical passwords may be a viable option. However, this has never been tested, so this thesis is the first step in addressing that gap.

Chapter 3

Password Systems

3.1 PassTiles

There are several kinds of graphical passwords for mobile as well as desktop devices. We chose a recognition based graphical password called PassTiles for our study as initial testing [45] [48] [46] shows that it is easy to understand and leverages the user's recognition memory to provide a more memorable password. It consists of square tiles in a grid based structure. Out of those tiles, a certain number of them that make up the user's password must be remembered. The user clicks on each of the tiles included in their password in order to successfully log in. The tiles can be clicked in any order. The theoretical password space of PassTiles depends on the total number of tiles in the grid and the number of tiles that make up the password. Passwords may be user chosen or randomly assigned by the system.

We used three different variants of PassTiles for our user study. Each had different memory cues so we could determine which one works best for both the child and adult age groups. For *Objects PassTiles*, we used images of different everyday objects as background images for each tile. *Image PassTiles* used one large image in the background with the tiles superimposed so it seemed like the image has been divided into a grid. Lastly, we used some simple and common 1-4 letter words as the background image for each tile in *Words PassTiles*. Details of each scheme are provided in section section 3.4.

Stobert et al. [45] proposed PassTiles as a graphical password that could be used to improve end user security while providing the user with better memorability by using recognition based passwords. PassTiles have been used in a user study by Stobert et al. [48] to examine how background images affect patterns and hot spots in user-chosen PassTiles. Stobert et al. [46] also examined the memorability and usability of different types of PassTiles as a recognition based graphical password by

comparing it with recall based graphical passwords and text passwords.

Wright et al. [57] conducted a study to determine if the use of recognition in text based passwords could improve their usability. In their study, a recognition based graphical password similar to the Words PassTiles was compared against recall based letter passwords as a retrieval mechanism. They found that the letter recall condition performed better than the recognition based graphical password made up of words.

3.2 Multiple Versatile Passwords (MVP)

MVP is a web based user testing framework for allowing websites to use diverse knowledge-based authentication schemes [10]. PassTiles is one of the several authentication schemes that have been implemented within MVP. It provides a web environment for users to test out password schemes available on MVP by logging into a certain website. MVP is implemented in JavaScript and PHP, with a MySQL database storing detailed usage logs including cleartext passwords and user inputs. The system is extensively instrumented for research purposes and is not intended for actual deployment with real user accounts due to these logging capabilities.

MVP allows a user to train for any specific password system through a Password Trainer interface which can be set up by the researcher through the control panel. For each username entered in the control panel by the researcher, a host website is chosen as a test environment for the password scheme, the password scheme is selected and its configuration parameters are applied. The researcher conducting the study on that password scheme is in charge of creating a unique user ID for each participant through the control panel while setting up the desired parameters to generate the password scheme in the desired web environment. In our case, we opted to use only the Password Trainer as the host website.

By entering the username in the Password Trainer and clicking on the Create button, the password scheme is launched in a separate window according to the specifications entered earlier through the control panel. The researcher can track the participants' interactions with the password scheme though MVP's log listings. All interactions are time stamped, including the users' input and the system's responses.

The log data for a particular user includes the information from when the password

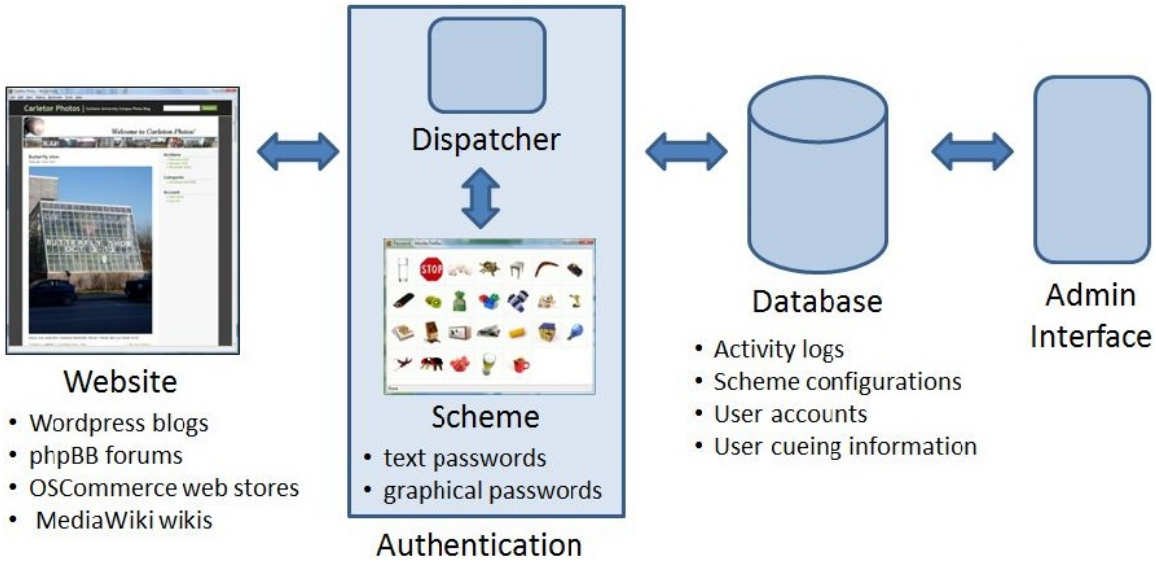

Figure 3.1: MVP Framework [10]

is generated till the user makes the last click to log in with their password. Additional log in sessions can be created by clicking on the Re-enter button in the password trainer to see if a user can log in with the same password after a certain period of time. The administrator is able to see whether a user enters the password correctly by clicking on the Check button in Password trainer. Figure 3.1 shows the basic flow structure of the MVP framework.

3.3 Changes made to the PassTiles UI

We made several adjustments to simplify the existing PassTiles interfaces to make them easier to use and understand for children. The previous interface showed a pop up message saying "Please practice your password by clicking on the highlighted squares". We changed this to display the message "Click OK to start". The researcher provided additional verbal instructions if needed. The previous interface also included the options to show or hide the password. We opted to always show the randomly generated password while it was being memorized.

There was a link which led the user to a tutorial in case they needed help. The link read "Click here for help using the password system". The tutorial was lengthy and intended for remote users. We removed the link from the interface and gave each

participant an in-person tutorial at the start of the session instead. Lastly, the button which allowed the user to log in with their password once it had been memorized was labelled "Password memorized-Continue". We changed the label of this button to "Start".

Image PassTiles allows users to select their own background image by flipping through a series of available images and selecting one. The previous interface had two buttons. One was labelled "Change picture" and it allowed the user to go to the next randomly selected picture. The other button, labelled "Choose this picture", allowed the user to select the picture as the background image for their Image PassTiles password. We relabelled these "Next picture" and "I like this picture".

The changes were made by logging into the MVP server and changing the HTML and JavaScript files for the PassTile system. Image PassTiles and Objects PassTiles had existing image sets on MVP. We filtered out images which would be inappropriate for children (e.g. wine, cigarettes, guns) and added new suitable images. We created a new image folder for Words PassTiles, storing all the words as images in jpg format. We used a total of 122 images for Words PassTiles, 200 images for Objects PassTiles and 322 images for the Image PassTiles.

3.4 Three PassTile Variants

For the study, we used three different variants the Passtiles password scheme: Objects, Image and Words. The MVP server was used to generate the passwords and monitor the user's performance. Examples of each are available in Figures 3.2-3.4. Each password scheme had 48 square tiles in an 8×6 grid. Five tiles were selected randomly by the system as the user's assigned password. The total number of possible combinations of passwords would then be $\binom{8\times6}{5}$. This gives us a password space of $log_2\binom{8\times6}{5}$ which is 21 bits. Florencio and Herley [23] suggest that 20 bits of password space is sufficient for online sites where secondary security mechanisms are present. Using this as a guideline, we choose a password space of 21 bits for this study. Since passwords were randomly assigned, no reduction in password space was caused by user choice; the full theoretical password space was used.

Memorization The five tiles that make up the password are highlighted with a red border at the start to allow the user to memorize them. The user can practice with the password by clicking on the tiles. Each correct tile turns blue when clicked. On completion of five successful clicks, a pop up message indicates that the user entered their password successfully. The Objects and Words PassTiles are shuffled for every successful password entry.

Login Once the user clicks the start button, a pop up message asks the user to enter their password. The red outlines will no longer be visible and the user will have to click on the five tiles they memorized previously. As the user clicks each of the tiles, they will not get highlighted to protect the password from shoulder surfing. The user is able to monitor the number of clicks made through a counter below the grid showing five small circles which change color incrementally on each click. The system allows duplicate clicks, counting them as two separate inputs. In case a user makes a mistake by clicking on the wrong tile, they can correct the mistake by clicking on the Clear button which will reset the password input and the user can re-enter it from the start. For this study, the order in which the participants click the tiles does not matter.

3.4.1 Objects PassTiles

The tiles in this password scheme consist of simple common objects used in everyday life. For each password entry, the password objects are shuffled so the user has to find the objects that make up their password from among all the other objects. Each object tile is displayed as an 80×80 pixel image with a light gray background. Figure 3.2 shows the graphical interface for Objects PassTiles during the memorization phase.

3.4.2 Image PassTiles

For Image PassTiles (Figure 3.3), a user first chooses an image to use as a background for the PassTile password. Once a user selects the image, it gets superimposed with a grid. Five tiles from the grid are selected as the users' password. The user will have to remember those five location in the image and can use the contents of the

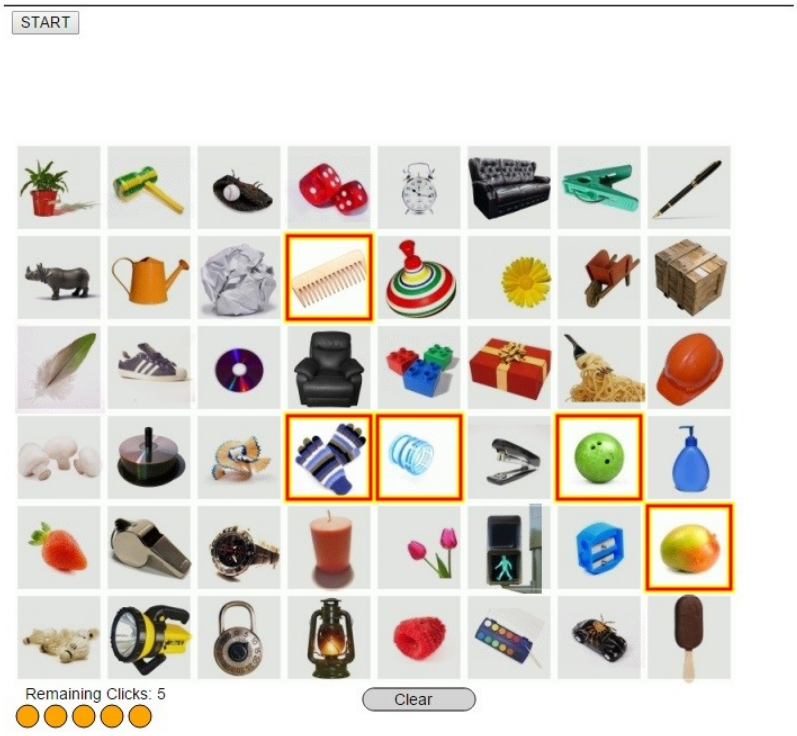

Figure 3.2: Objects PassTiles during memorization phase

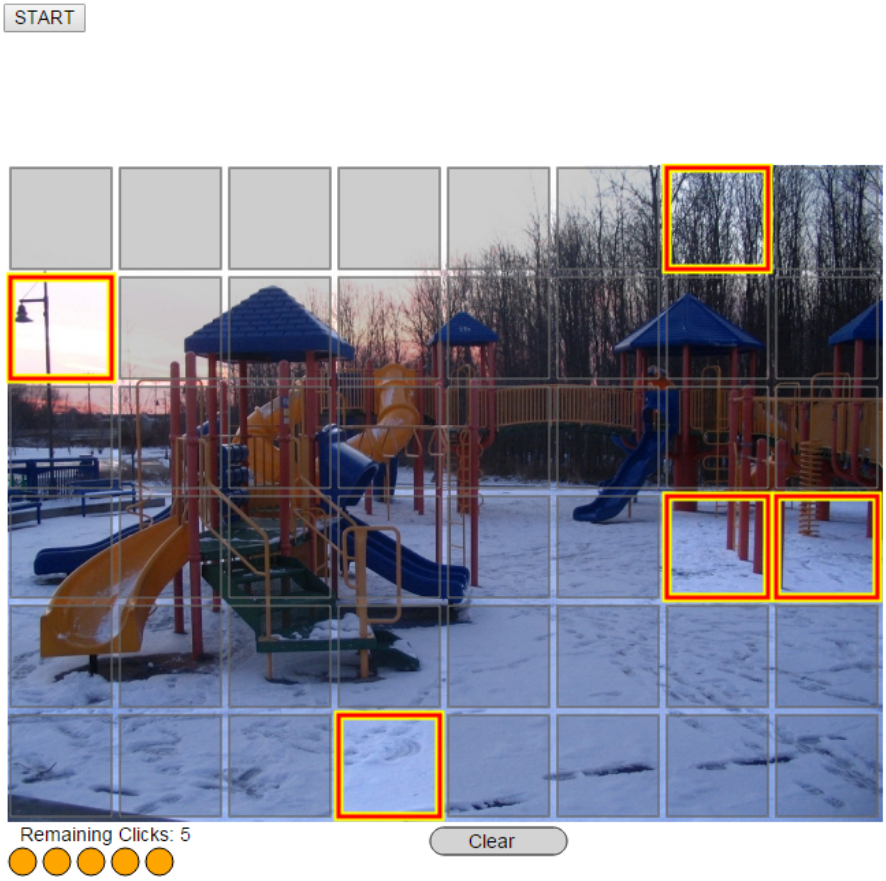

Figure 3.3: Image PassTiles during memorization phase

background image to help in memorizing the password. Each image is 640 × 480 pixels in size which gets divided into 80 × 80 pixel tiles. All images are photographs consisting of different places, people, buildings, animals or landscapes. Due to the nature of the visual cue, tiles are not shuffled in this variant.

3.4.3 Word PassTiles

Similar to Wright et al.'s scheme [57], we introduced a new PassTile variant to the system called Word PassTiles (Figure 3.4) which consists of one to four character words. We wanted to keep the words as simple as possible so that children would find the words easy to read. The words were created as jpg images using Microsoft PowerPoint and then transferred to the images folder in the MVP database to be used as Words PassTiles. The words mostly consist of nouns but there are also verbs,

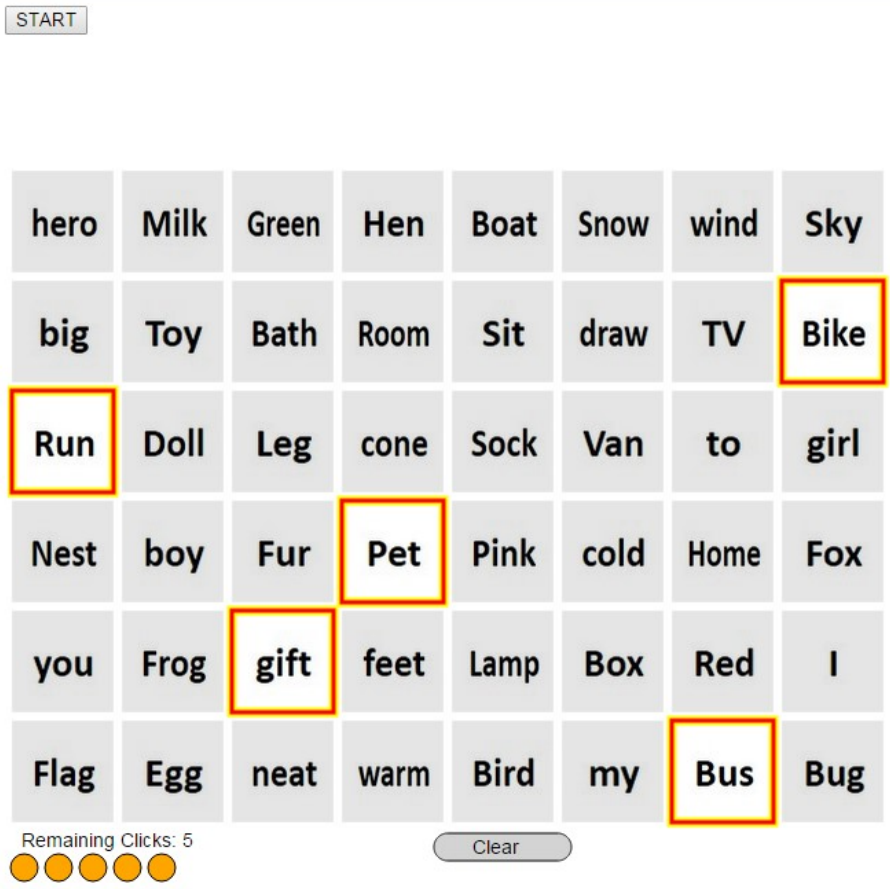

Figure 3.4: Words PassTiles during memorization phase

adjectives, pronouns, articles and prepositions. All the words are in black font on a light grey background. All word images are 80×80 pixels in size and shuffled with every login.

Chapter 4

Methodology

4.1 Study Design

We conducted two user studies, one with children and one with adults. The goal was to compare the performance of children against adults when it comes to password memorability and recognition while using graphical passwords. We used three graphical password schemes based on PassTiles, namely, Objects, Image and Words PassTiles and each participant tested all three schemes. For both studies, we used a balanced presentation order for the password schemes to ensure that results are not biased on the order of presentation. As there were three password schemes, this resulted in a total of six different combinations of those schemes. Each participant was presented with a different combination and the same combinations were repeated after every six participants. Both studies were reviewed and cleared by the Carleton University Research Ethics Board (CUREB).

4.2 Procedure

For the first user study, the goal was to evaluate the performance and interaction of children with each of the three graphical password schemes. The participants created a password for each of the three passwords schemes and then entered that password when prompted. We monitored the children throughout the study and observed their interaction with Object, Image and Words PassTiles. We briefly interviewed parents for contextual information. In the second study, we monitored the interaction of adults with the same three passwords using the same methodology as the first study. Sessions lasted on average 25 minutes for children, 6 minutes for parents and 18 minutes for adult participants. Each child and parent participant received a $10 gift card from the Chapters bookstore as compensation for participating in the user study.

Adult participants received $10 in cash.

4.2.1 Phase 1: Consent and Introduction

This initial phase varied between the two studies to accommodate the two groups of participants. We describe both procedures.

Children Study: Before starting the study, the parents were given two consent forms to sign. One was for the parent themselves, stating that they agree to participate in the study and explaining the parent interview portion of the study. They were also asked for permission to audio record the interview. The form clearly stated that the research project had been reviewed and received clearance from the Carleton University Research Ethics Board. The form also stated that the participants had the right to decline answering any of the questions or withdraw from the study at any time without providing any justification. They would receive a $10 gift card from Chapters for participating in the study even if they withdrew.

The second consent form asked the parents to give permission for their children to participate in the research. It explained what their child would be asked to do throughout the study. It explained that the child must also agree to participate otherwise they would not be included in the study. Parents were politely asked not to be mad at their children or force them to participate if they did not wish to do so. Permission was asked from the parents to allow their children to be audio-recorded during the study. Any child could withdraw from the study at any time and they would still receive a $10 gift card from Chapters for participating. The parents were also given a demographic questionnaire to fill out to get some information about themselves and their children.

The children were then asked for verbal consent, with the experimenter explaining to them what they would be doing throughout the study and asking whether they wished to take part. They were also asked for permission to audio record the session.

Adult Study: The adults were presented with a consent form before the start of the study. This consent form explained what they would be doing in the study and

also asked for their permission to audio record the session. After consenting, the adult participants were given a demographic questionnaire to fill out so we could gather information about them as well as assess their knowledge and experience with passwords.

Introduction: We explained to the participants what tasks they would be performing throughout the study by showing them printed snapshots of the three password schemes and explaining verbally how the system worked and how they would enter their passwords once they were memorized.

4.2.2 Phase 2: Memorize Password

Phases 2 and 3 were repeated three times, once for each type of password scheme; users completed the memorization (Phase 2) and first login (Phase 3) for one variant before moving on to the next. Participants memorized the password presented on the screen. This password consisted of five tiles selected randomly by the system and highlighted in red. The participants could practice entering their password to see how the system works and what happens once a password is entered correctly or incorrectly. This was meant to be a training and memorization exercise and users could take as long as they wanted. Passwords were system-assigned, therefore, users had no choice in selecting their password, other than selecting their background in the Image PassTiles variant. Once they had memorized the passwords, they were asked to click the start button to use that password to complete the first login.

4.2.3 Phase 3: First Login

Participants logged into the system using the newly memorized password. On clicking the start button they were presented with the PassTiles interface but this time none of the tiles were highlighted in red. Participants received no feedback about which tiles they clicked. However, the counter at the bottom of the image incremented with each tile clicked, to a maximum of five. For the Objects and Words passwords, the tiles were shuffled. This was done to make sure that the password remained completely recognition based and the participants did not use the location as cues while logging

in. The participants clicked on the tiles which they thought composed their password and once they had made five clicks their password was either accepted or rejected. Users were given the chance to login only once for each variant.

4.2.4 Phase 4: Interview

After completing first logins with all three variants, we asked participants some questions regarding their opinions of all three password variants. The interview consisted of 15 questions and lasted for an average of 12 minutes. All interviews were audio recorded to provide us with a better insight of the participants' views of the different password schemes. Through the interview, we gathered information like which of the three password schemes the participants liked most, which one was the most difficult, and which password scheme was most secure in their opinion. We also asked questions regarding their current password practices and how they remember passwords. There was an extra question for the children, asking who taught them to create passwords.

4.2.5 Phase 5: Second Login

Participants were asked to re-enter their three passwords after the interview. All three passwords were presented in the same order as in first login. To test memorability, participants had one attempt per variant. This was done to see whether the participants would remember their passwords after a brief interruption. Tile highlighting was off, so participants received no feedback about which tiles were selected; only the counter at the bottom left of the screen incremented with each tile clicked.

4.2.6 Phase 6: Parent Interview

The parents of the children were interviewed after the children were done re-entering their passwords. As many of the child participants were siblings accompanied by a single parent, we had each child in the family complete the user study before interviewing the parent. Parents were asked questions about their children's online privacy and security like how much time they allowed their children to spend online, whether they monitored their children's online activity and what steps they took to make sure that their children are safe when they spend time online.

4.3 Environment and Equipment

The adult study took place in a Carleton University research lab in a peaceful environment with no outside interference. The child study took place in two different environments. Eight children completed the study in the lab and seventeen children completed it in an Ottawa public library. We asked the parents to bring them to the closest library for their convenience. We selected a spot within the library which was quiet and peaceful to set up the study to avoid distraction.

We used a Sony VAIO laptop with a touch-screen and running Windows 8. The participants were requested to use a mouse to enter their input but in case they found it hard to enter by using the mouse, they could switch to touch input. This was particularly meant to help the younger children to enter their passwords as using the mouse could prove difficult for them; only three children used the touch-screen.

4.4 Child and Parent Participants

We recruited 25 child participants between the ages of 7 and 12, with an average age of 9.5 years. Ten were male and the remaining fifteen were female. All children were accompanied by a parent. Ten participants had experience using PINs to unlock tablets or smartphones. Nine used alphanumeric passwords consisting of both letters and numbers while six used simple text passwords consisting only of letters to unlock a computer or laptop. Two participants had experience using a grid pattern password to unlock their phones. One participant had no experience with using passwords. Of those with experience, twenty participants had been taught by their parents to create passwords while two learned by themselves and two from their older siblings.

There were eleven parents in total that accompanied the children, all of them female. Seven of the parents were between the ages of 30 to 40 years while four were between 41 to 50 years of age. Six were stay-at-home parents who were home-schooling their children and five had jobs in different professions. Five parents had a college diploma, three had a Bachelors degree, two had a Masters degree and one had a high school diploma.

4.5 Adult Participants

We recruited 25 adult participants for our study to match the number of child participants. Twenty were university students studying in different programs, three were working full-time and two were unemployed. Eight participants were between the ages of 18 and 20 years, twelve were between the ages of 21 and 30 years and five were over the age of 30. Fourteen participants were male and the remaining eleven female. Five participants had a high school diploma, twelve had a Bachelors degree, six had a masters degree and two had a doctoral degree. All participants were familiar with the use of passwords and had experience using multiple passwords for different online accounts.

Chapter 5

Analysis and Results

In this chapter, we present the data collected from our studies. Before analysing the data, we propose several hypotheses and then conduct statistical tests to see whether they are supported. We analyse the data in three major categories: login success rates, degree of correctness, and login time. For each of these data categories, we measure the effect of age group (children versus adults) and the effect of scheme and formulate the results accordingly.

5.1 Hypotheses

Prior to our analysis, we formed the following hypotheses with respect to our data:

H1: Adults will outperform children in all three graphical passwords (Objects, Image and Words PassTiles).

Ho: Adults and children perform equally well in each password scheme.

H2a: Children will have highest performance with Objects PassTiles.

Ho: Children do equally well in all three password schemes.

H2b: Adults will have highest performance at Words PassTiles.

Ho: Adults do equally well in all three password schemes.

H3: Children will prefer graphical passwords to other types of passwords.

Ho: Children prefer graphical and other passwords equally.

H4: Children will have a greater liking to graphical passwords as compared to adults.

Ho: Children and adults prefer graphical passwords equally.

H5a: Children will have a higher opinion of Objects PassTiles.

Ho: Children have equal opinion of all three password schemes.

H5b: Adults will have a higher opinion of Words PassTiles.

Ho: Adults have equal opinion of all three password schemes.

5.2 Analysis Plan

Our study design has one independent factor (age: adults and children groups) and one repeated measures factor (scheme: each participant tested all three PassTiles variants). As no standard test exists for non-parametric mixed factorial designs, we tested each factor independently, with corrections as appropriate. We used seven different statistical tests for the analysis of the data acquired through our studies:

Chi-Square Goodness of Fit Test This test is used to determine whether observed sample frequencies differ significantly from expected frequencies specified in the null hypothesis. It is used to determine whether sample data are consistent with a hypothesized distribution. We used it to compare the participants' preferences for type of scheme against equally distributed selections of each sample size. It is a non-parametric test used to compare the independent data obtained from the interview results of participants. It has been used to compare 2-3 different groups.

Fisher's Exact Test This test is used when you have two nominal variables and you want to see whether the proportions of one variable are different from those of the other variable. It is more accurate than the chi-square test when the sample size is small. This is also a non-parametric test used with independent data. We use it to compare adults and children's login success and interview results.

Unpaired T-test The unpaired t-test compares the means of two independent sample groups, assuming that the values follow a Gaussian distribution. The t-test determines a probability that two populations are the same with respect to the variable tested. It is a parametric test and we used it to compare the login time between adults and children for each password scheme.

Mann Whitney U Test It is used to test whether two independent samples of observations are drawn from the same or identical distributions. It is a non-parametric test that allows two groups to be compared without making the assumption that values are normally distributed. In order to calculate the U statistics, the combined set of data is first arranged in ascending order with tied scores receiving a rank equal to the average position of those scores in the ordered sequence. We used it in comparing the degree of correctness for each login between adults and children.

Friedman Test The Friedman test is a non-parametric test that compares three or more paired groups. The Friedman test first ranks the values in each matched set (each row) from low to high. Each row is ranked separately. It then sums the ranks in each group (column). If the sums are very different, the p-value will be small. It is used for one-way repeated measures analysis of variance by ranks. We have used it in comparing the degree of correctness between the three passwords schemes for each login attempt.

Repeated Measures ANOVA This test detects any overall differences between related means. This usually occurs in two situations: (1) when participants are measured multiple times to see changes to an intervention; or (2) when participants are subjected to more than one condition and the responses to each of these conditions are to be compared. Our data falls in the second category. This particular test requires one independent variable and one dependent variable. The dependent variable needs to be continuous (interval or ratio) and the independent variable categorical. We used this parametric test to compare the login time among the three password schemes for each login attempt.

Cochran's Q Test This non-parametric test is used to statistically analyse success rate data between three or more matched sets of frequencies. Cochran's Q can test whether the responses across the conditions are significantly different from each other. The response variable can take only two possible outcomes 0 (unsuccessful) and 1 (successful). We use it to compare the login success rates among the three password schemes for each login attempt.

McNemar's Test This non-parametric test is used on paired nominal data. It is applied to 2 x 2 contingency tables with matched pairs of subjects, to determine whether the row and column marginal frequencies are equal. We used it as a post hoc test to Cochran's Q test to compare the password schemes while analysing login success rates.

Tukey's Test This test uses a multiple comparison procedure in conjunction with an ANOVA (Post-hoc analysis) to find means that are significantly different from each other. It compares all possible pairs of means and identifies any difference between two means that is greater than the expected standard error. We used it as a post hoc test to compare the login times across password schemes.

Bonferroni Correction This method is an adjustment made to p-values when several dependent or independent statistical tests are being performed simultaneously on a single data set. It reduces the chances of obtaining false-positive results (type I errors) when multiple pair wise tests are performed on a single set of data. We perform Bonferroni correction for each of our post-hoc tests by dividing the original p-value of 0.05 by 3 which is the number of schemes we compare. The statistical power of the study is then calculated based on this modified p-value of 0.0167.

P-value The p-value is the probability of observing a sample statistic as extreme as the test statistic. The degrees of freedom (DF) is equal to the number of levels (k) of the categorical variable minus 1: $DF = k - 1$. For all our hypotheses, we used $p < 0.05$ as the threshold for statistical significance. For each of our hypotheses, we state a null hypothesis (Ho).

5.3 Login Success

We measured login success at two points during the session. The first login attempts occurred immediately after memorizing each password. The second login attempt happened at the very end of the session, after we were done interviewing the participant. We report the success rates for adults and children per scheme. Participants

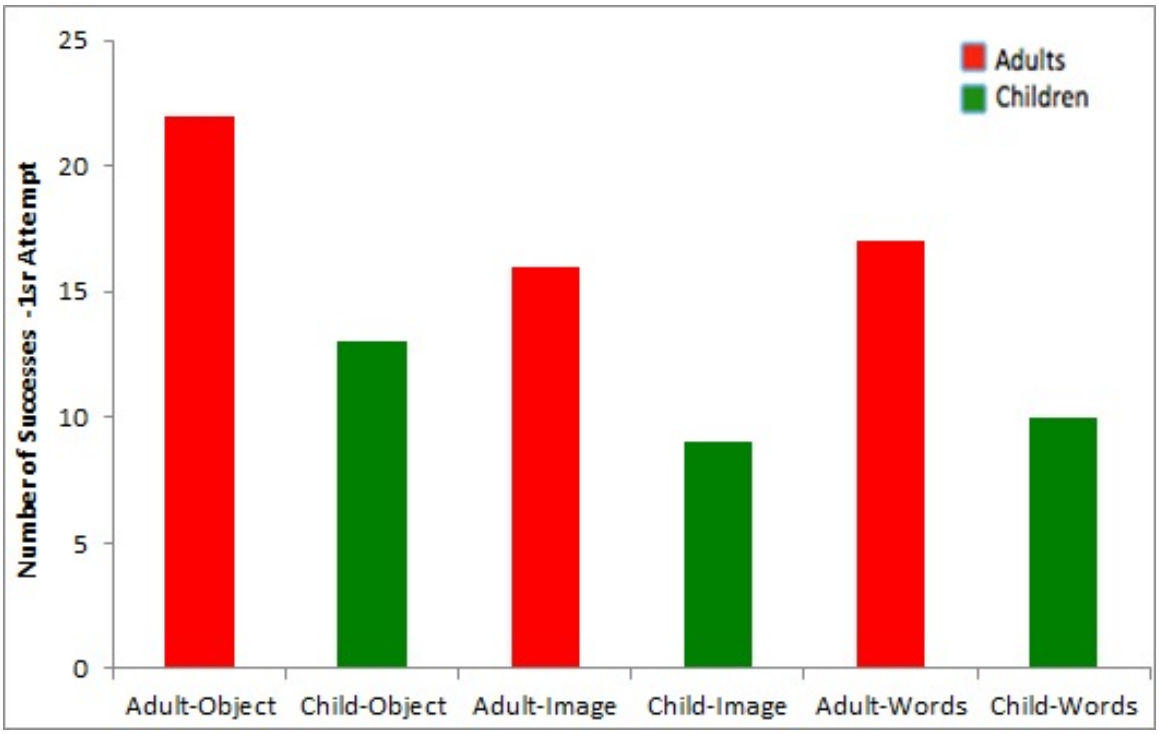

Figure 5.1: First Login: number of participants who successfully logged in out of 25 participants per group

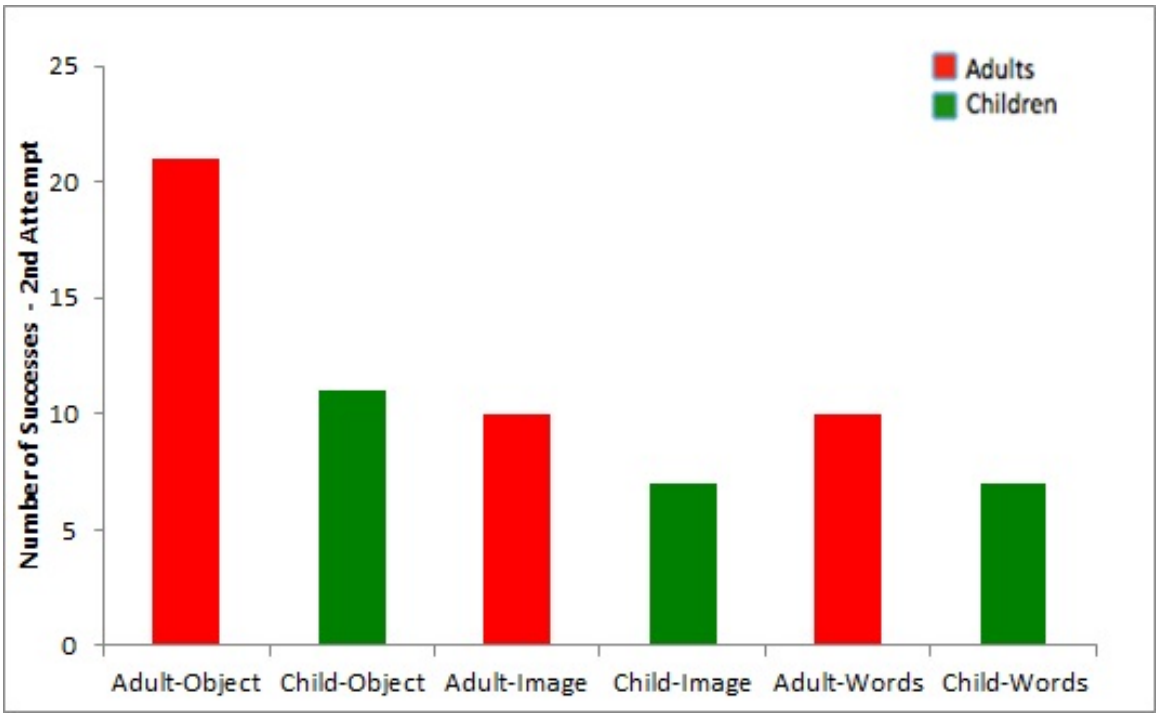

Figure 5.2: Second Login: number of participants who successfully logged in out of 25 participants per group

had only one try to enter their password for each login attempt and the result was identified as success or fail. Figure 5.1 and 5.2 illustrate the number of participants who were successful at logging in at each attempt.

Overall, we can observe that a greater number of adults are successful in logging in correctly for both login attempts as compared to children. The number of successes for Objects PassTiles remains high in both login attempts for adults however it drops considerably for Image and Words PassTiles during the second attempt. The number of successes for children drops slightly in the second login attempt with the most successes in Objects PassTiles for both logins.

5.3.1 Effect of Age

A two-tailed Fisher's exact test was used to compare the success rates of adults and children using the Objects, Image and Words PassTiles for the first and second login attempts.

First Login

Objects PassTiles The test gave a p-value equal to 0.0121, hence the results were statistically significant and the null hypothesis was rejected. Adults perform better than children while using the Objects PassTiles.

Image PassTiles The test gave a p-value of 0.0887. This value is above a P of 0.05, hence the results are not statistically different and the null hypothesis could not be rejected. No statistically significant differences were observed between adults and children for successful first login with Image PassTiles.

Words PassTiles The test gave a p-value of 0.0877, hence the results are not statistically different and the null hypothesis could not be rejected. Adults and children performed similarly.

Second Login

Objects PassTiles The test gave a p-value equal to 0.0072, hence the results were statistically significant and the null hypothesis was rejected. Adults were better able to remember their Objects PassTiles passwords than children during the second login.

Image PassTiles The test gave a p-value of 0.5512, hence the results were not statistically different and the null hypothesis could not be rejected. Both adults and children remembered their Image PassTiles password poorly during the second login.

Words PassTiles The test gave a p-value of 0.5512, hence the results were not statistically different and the null hypothesis could not be rejected. Adults and children both had difficulty remembering their Words PassTiles passwords.

As the results of the Fisher's Tests show, adults performed better than children when using Objects PassTiles for both login attempts. The performance of adults and children was quite similar for Image and Words PassTiles during both login attempts.

5.3.2 Effect of Scheme

For each participant group, we did an analysis on the success rates for each login attempt by comparing all three password schemes with each other using the Cochran's Q Test. Each login attempt was assigned a 0 (unsuccessful) or 1 (successful). The critical chi square value for this test was 5.99 with a degree of freedom of 2 and p-value of 0.05; therefore, chi square values greater than 5.99 are considered statistically significant.

First Login Children A Q value of 2.0 was calculated for this test which is less than the critical chi square value, hence the null hypothesis cannot be rejected. Children had difficulty remembering all three passwords for the first login attempt.

Second Login Children A Q value of 2.909 was calculated for this test which is less than the critical chi square value, hence the null hypothesis cannot be rejected. Children perform equally well in all three password schemes for the second login attempt.

First Login Adults A Q value of 4.133 was calculated for this test which is less than the critical chi square value, hence the null hypothesis cannot be rejected. Adults perform equally well in all three password schemes for the first login attempt.

Second Login Adults A Q value of 12.736 was calculated for this test which is greater than the critical chi square value, hence the null hypothesis is rejected. Significant differences were found for adults between the schemes for the second login.

We conducted a post hoc McNemar's test to find where these differences occurred. Using Bonferroni correction, we reduced the p-value to 0.0167. The p-values of each comparison can be seen in Table 5.1. We found differences between Objects PassTiles and the other schemes to be statistically significant. Objects PassTiles was significantly more memorable than the other schemes for adults.

Both adults and children had similar success rates when comparing within each group across the three password schemes during the first login. However, during the second login, adults had a significantly higher success rate in Objects PassTiles as

Comparison	p-value
Objects-Words	0.0034
Words-Image	1.0000
Objects-Image	0.0034

Table 5.1: Post hoc McNemar's test for Adults' second Login (Success Rates)

	Objects		Image		Words	
	Adults	Children	Adults	Children	Adults	Children
Minimum	80.0	0.0	40.0	0.0	80.0	20.0
25th Percentile	100.0	80.0	80.0	60.0	80.0	60.0
Median	100.0	100.0	100.0	80.0	100.0	80.0
75th Percentile	100.0	100.0	100.0	100.0	100.0	100.0
Maximum	100.0	100.0	100.0	100.0	100.0	100.0
Mean	97.6	83.2	88.8	68.8	93.6	80.0

Table 5.2: Degree of correctness for First Login attempt

compared to the other two schemes. The performance of adults in Objects PassTiles remained consistent for both login attempts whereas it deteriorated for Image and Words PassTiles in the second attempt. No differences were found in the second login for children.

5.4 Degree of Correctness

To more closely assess participants' ability to remember their passwords, we examined the number of correct tiles remembered per password. The degree of correctness ranges from 0-100 percent, indicating the number of tiles out of 5 that were successfully remembered. For example, 40 percent correctness means that 2 out 5 tiles were remembered.

The degrees of correctness for first login attempt can be seen in Figure 5.3 and Table 5.2. The degrees of correctness for the second login attempt are in Figure 5.4 and Table 5.3. We see that the degrees of correctness are generally high, particularly for first attempt, which is expected given that participants had just memorized their password. There is more variance for the second attempt. In both attempts, we observe higher variance for children than adults. Percentages are reported for easier comparison, but all statistical tests used actual counts of the number of correct tiles.

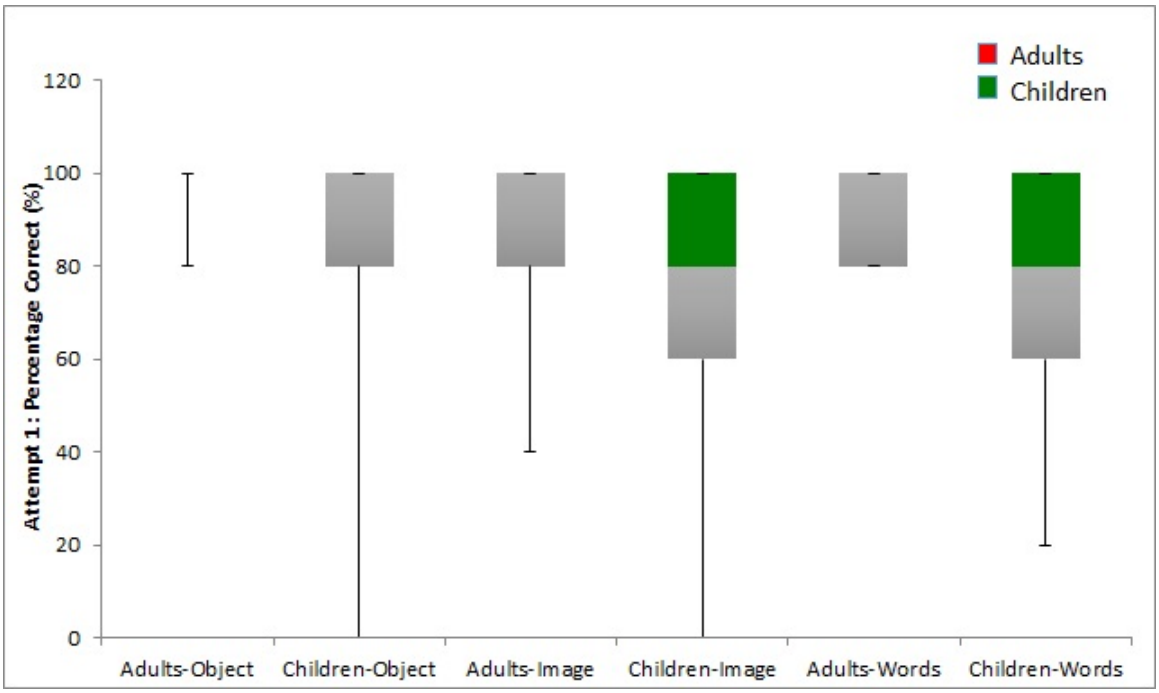

Figure 5.3: Degree of correctness for First Login Attempt

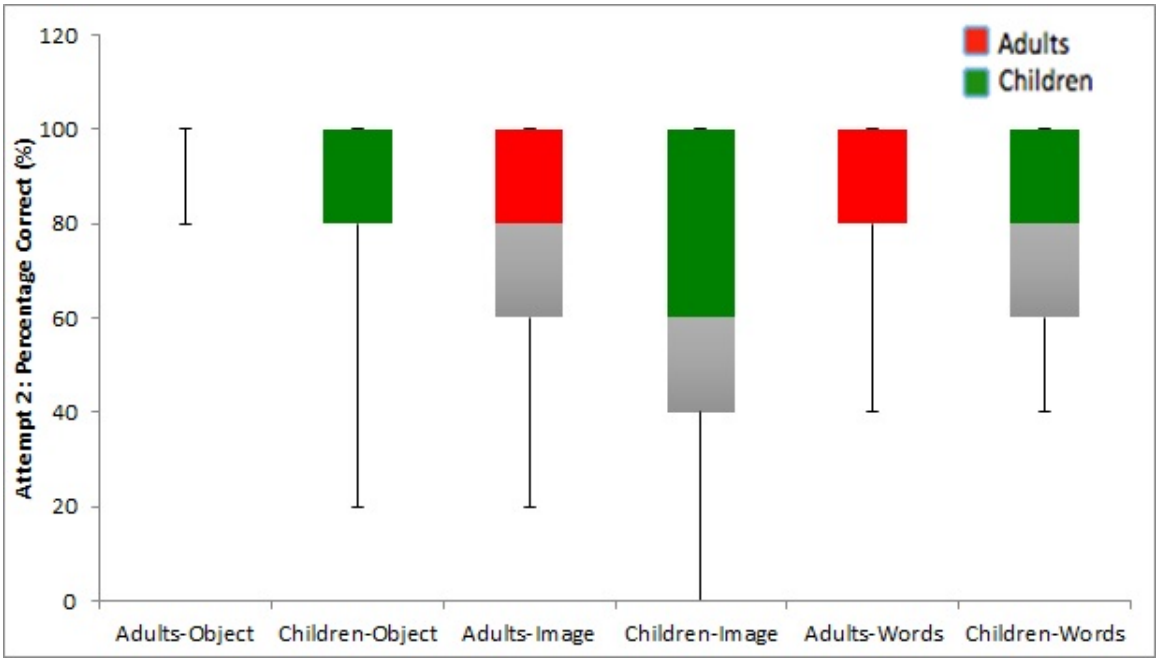

Figure 5.4: Degree of correctness for Second Login Attempt

	Objects		Image		Words	
	Adults	Children	Adults	Children	Adults	Children
Minimum	80.0	20.0	20.0	0.0	40.0	40.0
25th Percentile	100.0	80.0	60.0	40.0	80.0	60.0
Median	100.0	80.0	80.0	60.0	80.0	80.0
75th Percentile	100.0	100.0	100.0	100.0	100.0	100.0
Maximum	100.0	100.0	100.0	100.0	100.0	100.0
Mean	96.8	81.6	79.2	64.8	83.2	72.0

Table 5.3: Degree of correctness for Second Login attempt

5.4.1 Effect of Age

We compare the degree of correctness between children and adults. A two-tailed Mann Whitney U test was used to compare the degree of correctness of adults and children for the Objects, Image and Words PassTiles during each login attempt.

Objects First Login For this test, a Z-value of 2.3186 was obtained and a U-value of 192.5 was calculated. Since, the distribution was approximately normal, the Z-value was used to calculate a p-value of 0.02034. This means that the result is significant and the null hypothesis was rejected. Adults outperform children while using Objects PassTiles during first login.

Objects Second Login The Z-value of 2.6097 was obtained and a U-value of 177.5 was calculated with a p-value of 0.00906. This means that the result is significant and the null hypothesis was rejected. Adults also outperform children while using the Objects PassTiles password for the second login attempt.

Image First Login The Z-value of 2.2604 was obtained and a U-value of 195.5 was calculated with a p-value of 0.02382. This result is significant and the null hypothesis was rejected. Adults outperform children while using the Image PassTiles password during first login.

Image Second Login A Z-value of 1.494 was obtained and a U-value of 235 was calculated with a p-value of 0.13622. This means that the result is not significant and the null hypothesis could not be rejected. Adults and children perform equally

well in the second login attempt for Image PassTiles. From Figure 5.4, we see that participants in both groups had some difficulty remembering their Image PassTiles password at the end of the session even though adults performed significantly better on the first attempt.

Words First Login A Z-value of 2.3089 was obtained and a U-value of 193 was calculated with a p-value of 0.02088. This result is significant and the null hypothesis was rejected. Adults perform better than children in the first login attempt for Words PassTiles.

Words Second Login A Z-value of 1.7172 was obtained and a U-value of 223.5 was calculated with a p-value of 0.08544. This result is not significant and the null hypothesis cannot be rejected. Interestingly, adults and children performed equally in the second login attempt for the Words PassTiles scheme, even though adults scored higher on the first attempt.

Adults had a higher degree of correctness on four of the six login attempts. Given adults' more extensive experience with passwords and computers in general, this was an expected result. Perhaps more interesting is the fact that no significant difference was found between the two groups for Image and Words PassTiles' second logins. Adults' performance appeared to deteriorate between login attempts while the children's performance remained more constant, resulting in similar degrees of correctness by the end of the second session.

5.4.2 Effect of Scheme

We also compared the degree of correctness between schemes (Objects, Image, Words) for each group of participants. Since each participant completed each scheme, this is a within subjects comparison.

We took the number of correct tiles on each password entry (varying between 0 and 5) and conducted a Friedman test to see if the participants performed equally well in all three password schemes during each login attempt.

Comparison	p-value
Objects-Words	0.0025
Words-Image	0.4839
Objects-Image	0.0017

Table 5.4: Post hoc Wilcoxon test for Adults' second Login (Degree of Correctness)

Adults First Login For the first login attempt, we obtained a chi square value of 2.34 and the p-value of 0.3104. The null hypothesis could not be rejected and the adults do perform equally well in all three password schemes.

Adults Second Login For the second login attempt, we obtained a chi square value of 10.16 and the p-value of 0.0062. The results are significantly different and the null hypothesis was rejected. There are significant differences in how many tiles adults remembered per scheme at the end of the session.

As the null hypothesis was rejected, we conducted a post hoc Wilcoxon test to determine where the differences were. Using Bonferroni correction, we reduced the threshold p-value to 0.0167 by dividing the original value of 0.05 by 3 as there are three schemes to compare. In Table 5.4, we can see the p-value obtained for the comparisons of each pair. We found the differences between Objects PassTiles and the other schemes to be statistically significant, with a higher degree of correctness for Objects PassTiles.

Children First Login For the first login attempt, we obtained a chi square value of 2 and the p-value of 0.3679. The null hypothesis could not be rejected and the children perform equally well in all three password schemes.

Children Second Login For the second login attempt, we obtained a chi square value of 4.34 and the p-value of 0.1142. The null hypothesis could not be rejected; the children perform equally well in all three password schemes.

The degree of correctness remained consistent for children during each login attempt and there was no significant difference in performance while logging in with each password scheme. Most children partially remembered their passwords, typically having difficulty with one or two of their tiles. The adults' degree of correctness

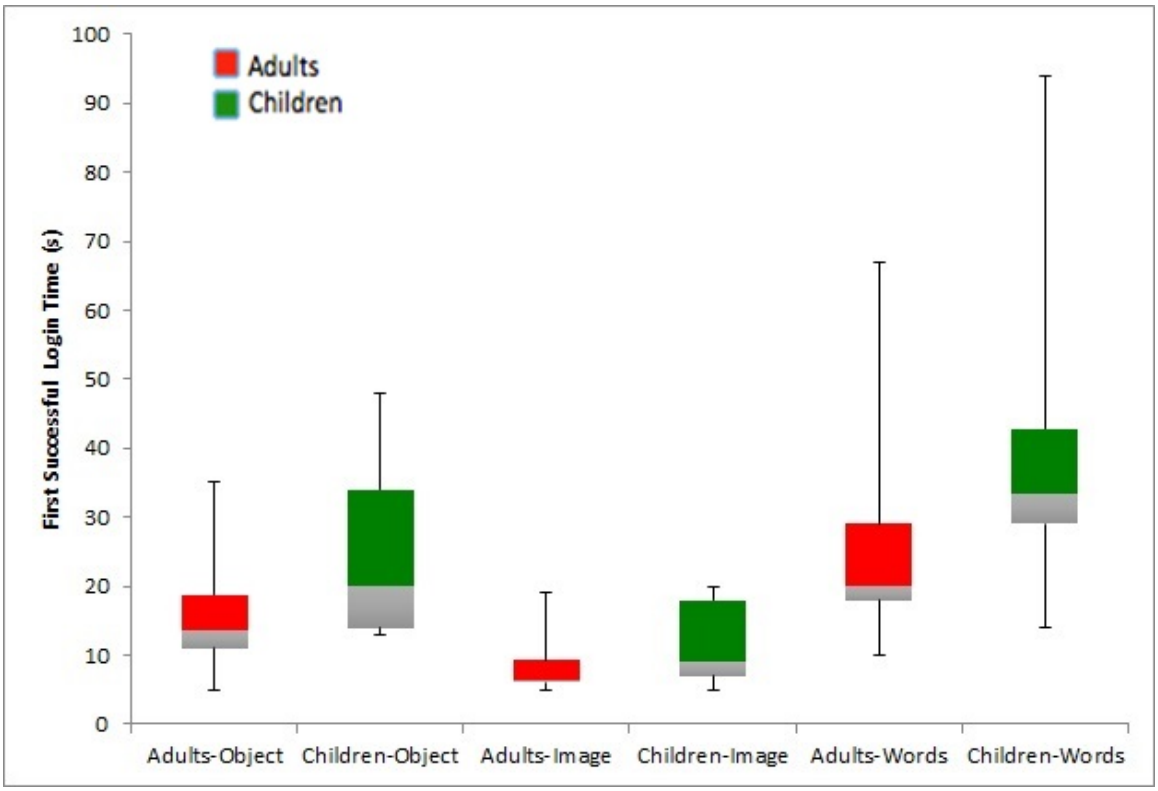

Figure 5.5: Login times for successful First Login Attempts

remained consistent for all three password schemes during the first login attempt. However, adults performed significantly better in the Objects PassTiles for the second login attempt as compared to the other password schemes. This indicated that while adults tend to forget their password for Image and Words PassTiles after a short time, they are more successful in remembering the Objects PassTiles password.

5.5 Login Time

Login time was measured as the time from when the login screen appeared to when the last tile was clicked. It is reported in seconds. We analyse successful logins and unsuccessful logins separately. Although the general trend observed is similar for the two cases, successful logins appear to have less variance in the time taken.

	Objects		Image		Words	
	Adults	Children	Adults	Children	Adults	Children
Minimum	5.0	13.0	5.0	5.0	10.0	14.0
25th Percentile	11.0	14.0	6.0	7.0	18.0	29.0
Median	13.5	20.0	6.5	9.0	20.0	33.5
75th Percentile	18.7	34.0	9.2	18.0	29.0	42.7
Maximum	35.0	48.0	19.0	20.0	67.0	94.0
Mean	15.2	24.2	8.4	11.8	26.2	38.6

Table 5.5: Login times for First successful login attempt in seconds

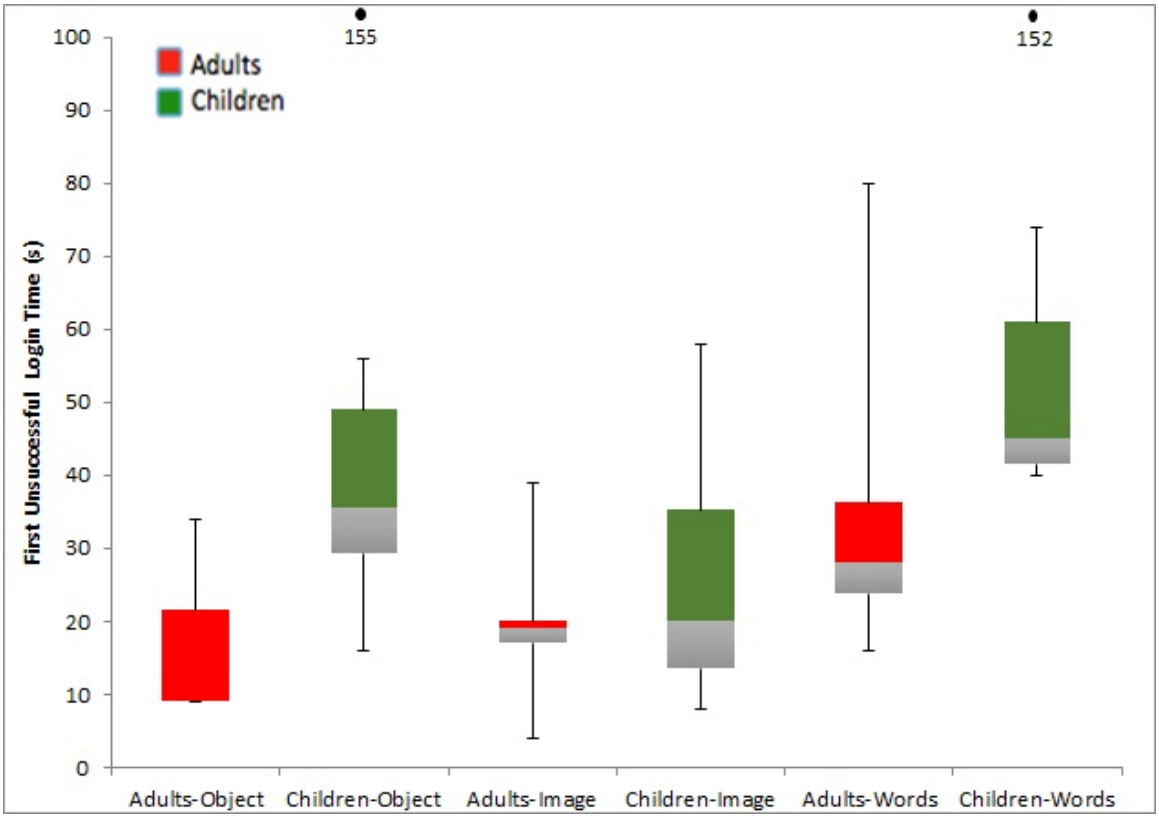

Figure 5.6: Login times for unsuccessful First Login Attempts

	Objects		Image		Words	
	Adults	Children	Adults	Children	Adults	Children
Minimum	9.0	16.0	4.0	8.0	16.0	40.0
25th Percentile	9.0	29.2	17.0	13.5	23.7	41.5
Median	9.0	35.5	19.0	20.0	28.0	45.0
75th Percentile	21.5	49.0	20.0	35.2	36.2	61.0
Maximum	34.0	56.0	39.0	58.0	80.0	74.0
Mean	17.3	38.2	18.6	25.6	34.0	51.2

Table 5.6: Login times for First unsuccessful login attempt in seconds

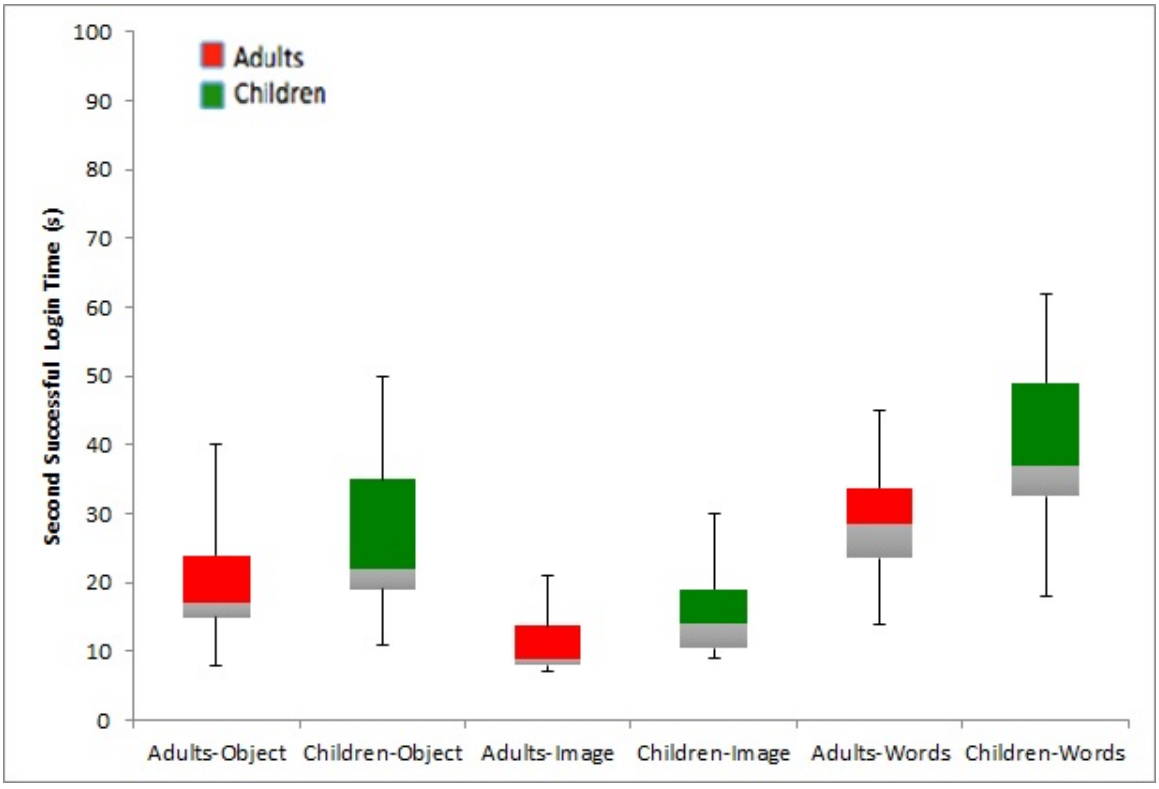

Figure 5.7: Login times for successful Second Login Attempts

	Objects		Image		Words	
	Adults	Children	Adults	Children	Adults	Children
Minimum	8.0	11.0	7.0	9.0	14.0	18.0
25th Percentile	15.0	19.0	8.0	10.5	23.5	32.5
Median	17.0	22.0	9.0	14.0	28.5	37.0
75th Percentile	24.0	35.0	13.7	19.0	33.7	49.0
Maximum	40.0	50.0	21.0	30.0	45.0	62.0
Mean	20.5	27.1	11.2	16.0	29.5	40.0

Table 5.7: Login times for Second successful login attempt in seconds

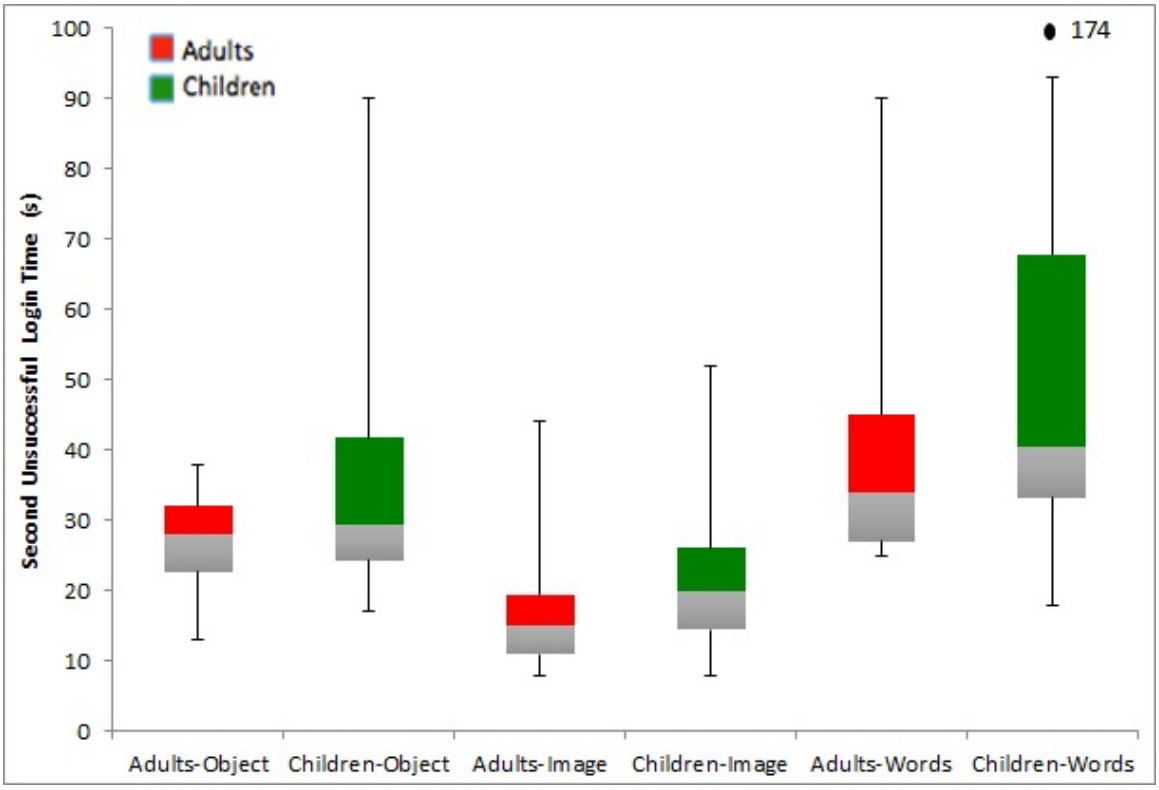

Figure 5.8: Login times for unsuccessful Second Login Attempts

	Objects		Image		Words	
	Adults	Children	Adults	Children	Adults	Children
Minimum	13.0	17.0	8.0	8.0	25.0	18.0
25th Percentile	22.7	24.2	11.0	14.5	27.0	33.2
Median	28.0	29.5	15.0	20.0	34.0	40.5
75th Percentile	32.0	41.7	19.5	26.0	45.0	67.7
Maximum	38.0	90.0	44.0	52.0	90.0	93.0
Mean	26.7	35.9	16.4	22.2	39.9	49.6

Table 5.8: Login times for Second unsuccessful login attempt in seconds

5.5.1 Effect of Age

An unpaired, two tailed t-test was used to compare the login times of the two attempts for children and adults in all three password schemes. Figures 5.5 to 5.8 show the login times for both adults and children for the two login attempts. Tables 5.5 to 5.8 illustrate the data for login times. As demonstrated in the following statistical results, children took significantly longer to login in all cases.

Objects First Login time The t-value calculated for the Objects first attempt was 3.428638 with a p-value of 0.001255, hence the results are statistically different. Login times for adults and children were different, with adults demonstrating quicker first login times for Objects.

Objects Second Login time The t-value for the second attempt was 2.780929 with a p-value of 0.007722, hence the results are statistically significant. Login times for adults were faster for the second login attempt as well.

Image First Login time The t-value for the Images first attempt was 2.70701 with a p-value of 0.009376, hence the results are statistically different. Again login times for adults were faster for the first login attempt for Image.

Image Second Login time The t-value calculated for the second attempt was 2.338956 with a p-value of 0.023548, hence the results are statistically significant. We found that adults were quicker for the second login attempt as well.

Words First Login time The t-value calculated for the Words first attempt was 3.676836 with a p-value of 0.000595, which are statistically significant. Login times were shorter for adults on the first login attempt with Words.

Words Second Login time The t-value for the second attempt was 2.41618 with a p-value of 0.019537, hence the two groups are statistically different. Once again, login times for adults were faster than children for the second login attempt.

Login Type	Objects-Words	Words-Image	Objects-Image
First Login-Children	$p < 0.01$	$p < 0.01$	n.s.
Second Login-Children	$p < 0.01$	$p < 0.01$	n.s.
First Login-Adults	$p < 0.01$	$p < 0.01$	n.s.
Second Login-Adults	$p < 0.01$	$p < 0.01$	n.s.

Table 5.9: Post hoc Tukey's tests for effect of scheme on login times, n.s. = not significant

5.5.2 Effect of Scheme

We conducted a Repeated Measures ANOVA test to compare the login times of the three password schemes per login attempt for each group. For this test, we calculated the degree of freedom DF (between) as 2 and the degree of freedom DF (Error) as 48. Taking these two DF values into account we get a critical value of 3.1826. We conducted these tests for both adults and children to see if there were any significant differences between the login times of the three password schemes.

For each test where the null hypothesis was rejected, we conducted a post hoc Tukey's Test to determine the level of significance of each password scheme. In the post hoc tests, we used the new p-value of 0.0167 calculated through the Bonferroni correction method. As detailed below, the statistical tests showed that in all cases the Word variant took significantly longer to login than the other schemes.

First Login times for Children An F-value of 19.14 was calculated and since this is greater than the critical value of 3.1826, the null hypothesis is rejected. The calculated p-value is less than 0.0001.

Second Login times for Children An F-value of 16.72 was calculated the null hypothesis is rejected. The calculated p-value is less than 0.0001.

First Login times for Adults An F-value of 18.49 was calculated and the null hypothesis is rejected. The calculated p-value is less than 0.0001.

Second Login times for Adults An F-value of 20.65 was calculated and the null hypothesis is rejected. The calculated p-value is less than 0.0001.

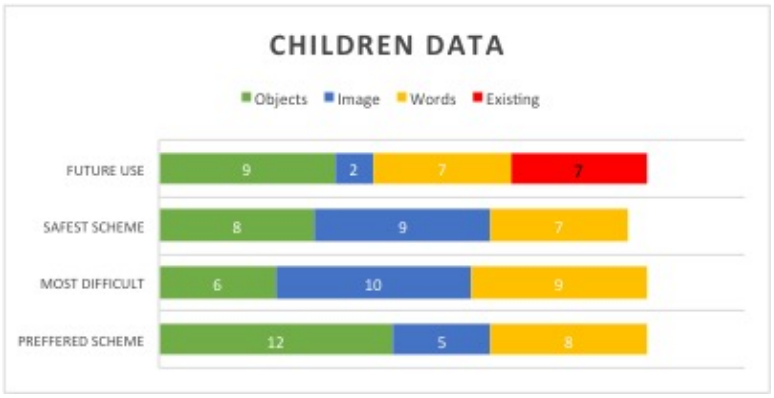

Figure 5.9: Number of children identifying each scheme in response to the interview questions

The results of all the post hoc Tukey's tests can be seen in Table 5.9. We can see that there is a statistically significant difference when comparing Words PassTiles to the other two password schemes. In all cases the Word variant took longer than the other two variants.

5.6 Preferences and Perceptions

We interviewed participants between the first and second logins to collect their preferences and perceptions of the schemes and passwords in general. We asked them four specific questions:

1. Would you like to use one of these different passwords instead of your regular one? If so which one? [Future Use]
2. Which of the passwords do you think is safest? [Safest Scheme]
3. Which one was the most difficult? [Most difficult]
4. Which type of password did you like the most? [Preferred Scheme]

For the first question, participants could choose their existing scheme or one of the three PassTiles schemes. For questions 2-4, they chose among the PassTiles schemes only. For each question, we tabulated the number of participants that identified a scheme in their response. Figures 5.9 and 5.10 summarize these responses for children and adults, respectively. One response from the children's data is missing because the participant said they did not know which scheme is safest.

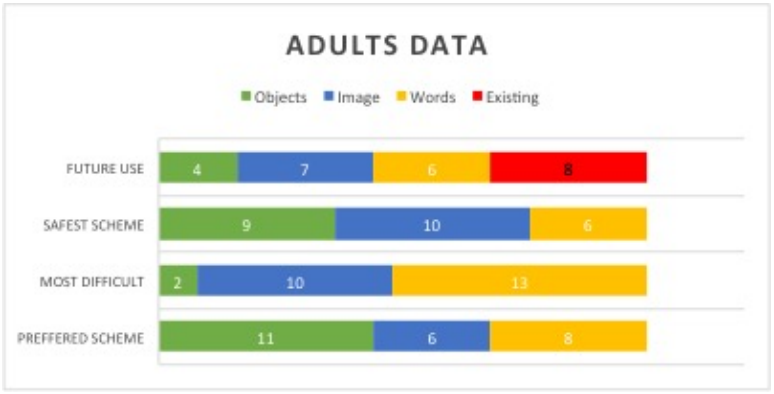

Figure 5.10: Number of Adults identifying each scheme in response to the interview questions

5.6.1 Future Use

We explored whether participants would prefer a graphical password when entering a new password as opposed to any of their existing schemes. We compared their actual preference to a distribution where graphical and existing schemes were equally preferred using a chi square goodness of fit test.

Effect of Scheme

Children: As shown in Figure 5.9, the number of children who agreed to have some variant of a PassTiles password for future use was a total of 18 (sum of the 3 PassTiles schemes) as opposed to 7 who wanted an existing scheme. A chi-square goodness of fit test was conducted to compare these two values with the expected values of 12.5 for each. The chi-square value of 4.840 was calculated with a p-value of 0.0278. This suggests that there is a significant difference and the null hypothesis was rejected. Children preferred graphical passwords to other types of passwords for future use.

Adults: As shown in Figure 5.10, the number of adults who agreed to have a PassTiles password for future use was a total of 17 (sum of the 3 PassTiles schemes) as opposed to 8 who wanted an existing scheme. A chi-square value of 3.240 was calculated with a p-value of 0.0719. These results are not significant and the null hypothesis could not be rejected. Although a preference for graphical passwords

seemed likely by looking at the graph, the statistical test revealed no difference when comparing to the expected value of 12.5 per group.

Effect of Age

We compared children and adults' responses. A two-tailed Fisher's exact test was used to compare the difference in future use of graphical versus existing types of passwords between adults and children. The two-tailed p-value obtained was 0.7536. Hence, the null hypothesis cannot be rejected. There were no statistically significant differences between groups with respect to preferred type of password for use in the future.

5.6.2 Safest Scheme

We asked the participants for their opinion on which password scheme they thought was the safest and would be the most difficult to guess or hack. The results from the interview question show that both the adult and child participants' opinion of the safest scheme was quite equally distributed among the three schemes.

Effect of Scheme

Children: A chi-square goodness of fit test was conducted to see whether the difference in participants' opinion of the safest PassTiles scheme was statistically different. We compared the observed values against the expected values of 8 for each scheme. The chi-squared value obtained was equal to 0.250 at 2 degrees of freedom. A p-value of 0.8825 was obtained. Hence the null hypothesis could not be rejected and children did not perceive any scheme to be safer than expected.

Adults: A chi-square goodness of fit test was conducted to see whether the difference in participants' opinion of the safest scheme was statistically different from the expected values of 8.33. The chi-squared value obtained was equal to 1.309 at 2 degrees of freedom. A p-value of 0.5949 was obtained. Hence the null hypothesis could not be rejected. Adults expressed no preference in terms of their perceived safest scheme.

Effect of Age

A two-tailed Fisher's exact test was used to compare the difference in opinion of safest scheme between adults and children. The two-tailed p-value obtained was 1.00. Hence, the null hypothesis cannot be rejected. There were no statistically significant differences between groups with respect to their opinion of the safest scheme.

5.6.3 Most difficult scheme

During the interview session, we asked participants about which scheme they found most difficult. Adults found Objects PassTiles to be least difficult, as can be seen in Figure 5.10. However, children had mixed opinions. We conducted a chi square goodness of fit test to compare the children's answers against the expected value in an equal distribution. A Fisher's Exact test was used to compare the adults' opinions of the most difficult scheme against expected values because of small observed values.

Effect of Scheme

Children: A chi-square goodness of fit test was conducted to see whether the difference in children's opinion of the most difficult scheme was statistically different from the expected values. The chi-squared value obtained was equal to 1.045 at 2 degrees of freedom with s p-value of 0.5930. Hence the null hypothesis could not be rejected. Children's responses did not differ from expected for most difficult scheme.

Adults: A Fisher's exact test was used to compare the observed values of 2 for Objects, 10 for Image and 13 for Words PassTiles against the expected values of 8.33 for each scheme. The two-tailed p-value obtained was 0.0820. Hence, the null hypothesis cannot be rejected. Adults think equally of all three schemes in terms of difficulty.

Effect of Age

A two-tailed Fisher's exact test was used to compare the difference in opinion of the most difficult scheme between adults and children. The two-tailed p-value obtained

was 0.333. Hence, the null hypothesis cannot be rejected. There were no statistically significant differences between groups with respect to their opinion of the most difficult scheme.

5.6.4 Preferred Scheme

We asked the participants which scheme they liked the most during the interviews. More participants favoured Objects PassTiles as compared to the other two schemes as can be seen from Figure 5.9 and 5.10. We conducted chi square goodness of fit tests to compare these values against the expected values of 8.33 for each scheme.

Effect of Scheme

Children: A chi-square goodness of fit test was conducted to see whether or not the difference in preferred PassTiles scheme were statistically different from expected values. The chi-square value obtained was 2.956 at 2 degrees of freedom. A p-value of 0.228 was obtained. The null hypothesis could not be rejected which means that children's preferences did not differ from the expected equal distribution of answers.

Adults: A chi-square goodness of fit test was conducted to see whether or not the difference in preferred PassTiles scheme were statistically different from expected for adults. The chi-square value obtained was 1.509 at 2 degrees of freedom. A p-value of 0.4702 was obtained. The null hypothesis could not be rejected which means that adults expressed no preference for any particular PassTiles scheme.

Effect of Age

A two-tailed Fisher's exact test was used to compare the difference in preferred scheme between adults and children. The two-tailed p-value obtained was 1.00. Hence, the null hypothesis cannot be rejected. There were no statistically significant differences between groups with respect to their preferred scheme.

5.7 Observations

We made several observation during the two studies. The children were mostly shy at the start of the session but as they played around with the first password scheme presented to them, they opened up more and asked more questions if they were confused. One question that was asked by three children was "Why can't we select our own boxes?" This suggests that the children were keen on making up their own passwords instead of having them pre-selected by the system. Adults, on the other hand, did not show any particular interest in making up a password of their own and asked fewer questions during the course of the study. A majority of the children showed great interest in the study and were highly motivated to perform their best. They were keen on learning how the passwords worked and frequently asked questions during the introduction phase of the study.

While picking an image for the Image PassTiles, children selected images that they found to be interesting, usually with animals or toys in them, but they did not focus on the rest of the content in that image such as whether it was diverse and would be easier to remember if divided into tiles. Most adults chose an image that they thought would be easier to remember with most of the content, and having a great variety of things in different locations. One child participant tried to remember the Image PassTiles password by counting the location of each tile using row and column number instead of using the background image as a cue.

Children had a hard time logging in with the Words PassTiles scheme. Words were harder for children to memorize and they tended to forget them more quickly. When it came to entering the password, they spent a longer time trying to recall what words made up their password. A couple of children who were 7 years of age could barely pronounce the words correctly. We encouraged the children to read the words out loud so they could remember them more efficiently. Several adult participants as well the older child participants tried to memorize the Words PassTiles password by forming a sentence out of the words which made up their password.

From Table 5.10 and 5.11, it can be seen that participants generally spent more time memorizing the passwords for successful login attempt. There is a fair amount of difference between the mean time taken to memorize passwords with successful

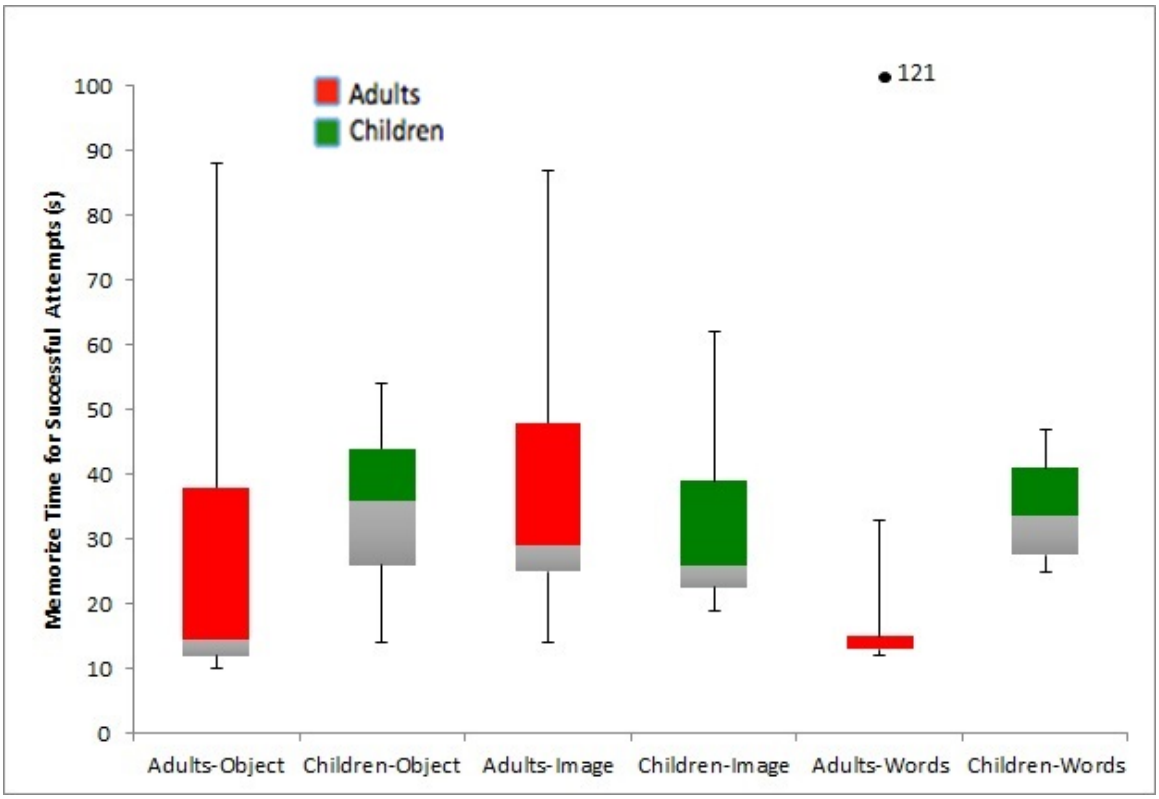

Figure 5.11: Memorization times for successful Attempts

and unsuccessful login attempts for both adults and children in Objects PassTiles. Figures 5.11 and 5.12 show the box plots of memorization times for successful and unsuccessful attempts. We counted every participant who was able to successfully log in during both login attempts as a successful attempt for these graphs.

Both adults and children made the mistake of clicking the same tile twice, thinking that it had not been clicked previously even though a green dot appeared in the click counter at the bottom left of the window. As the tiles do not get highlighted when clicked during login, a participant could forget which tiles have already been clicked. The participant might then think that they had entered the password correctly when in fact it was incorrect. This mistake was observed with eight adult participants and five child participants. A couple of participants also double clicked on the same tile without realising it. This is different from the previous error mentioned where the participant forgot they had clicked a tile. In this case, the participants were in a hurry to click the tiles and accidentally double clicked on one tile during the process.

	Objects		Image		Words	
	Adults	Children	Adults	Children	Adults	Children
Minimum	10.0	14.0	14.0	19.0	12.0	25.0
25th Percentile	12.0	26.0	25.0	22.5	13.0	27.5
Median	14.5	36.0	29.0	26.0	13.0	33.5
75th Percentile	38.0	44.0	48.0	39.0	15.0	41.0
Maximum	88.0	54.0	87.0	62.0	33.0	47.0
Mean	26.8	35.3	39.7	32.9	15.7	34.7

Table 5.10: Memorization times for successful login attempts in seconds

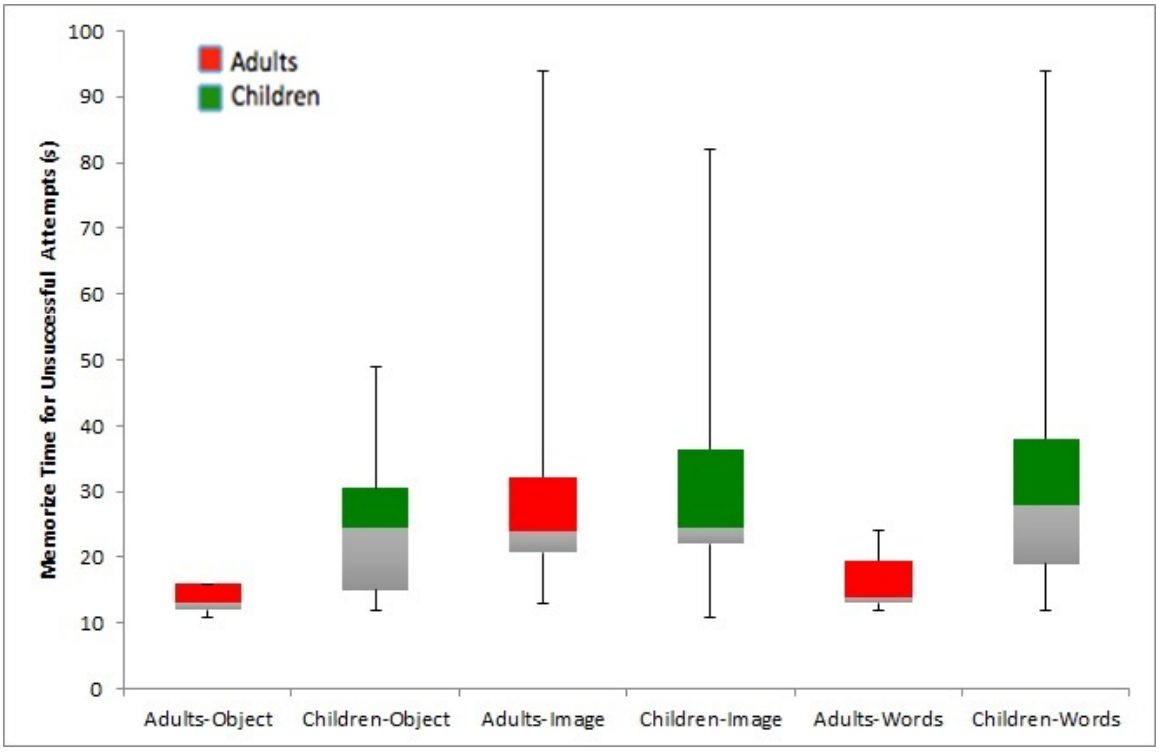

Figure 5.12: Memorization times for unsuccessful Attempts

	Objects		Image		Words	
	Adults	Children	Adults	Children	Adults	Children
Minimum	11.0	12.0	13.0	11.0	12.0	12.0
25th Percentile	12.0	15.0	20.7	22.0	13.0	19.0
Median	13.0	24.5	24.0	24.5	14.0	28.0
75th Percentile	16.0	30.5	32.2	36.5	19.5	38.0
Maximum	16.0	49.0	94.0	82.0	24.0	94.0
Mean	13.6	24.9	30.0	30.7	16.1	31.9

Table 5.11: Memorization times for unsuccessful login attempts in seconds

	Hypotheses	Support
H1:	Adults outperform children in all three graphical passwords	Partially Supported
H2a:	Children have highest performance with Objects PassTiles	Not Supported
H2b:	Adults have highest performance at Words PassTiles	Not Supported
H3:	Children prefer graphical passwords to other types of passwords	Supported
H4:	Children have a greater liking to graphical passwords compared to adults	Not Supported
H5a:	Children have a higher opinion of Objects PassTiles	Not Supported
H5b:	Adults have a higher opinion of Words PassTiles	Not Supported

Table 5.12: Support for Hypotheses

5.8 Support for Hypotheses

Table 5.12 summarized our hypotheses and whether our results offered support for each. We discuss each hypothesis next.

H1 This hypothesis is partially supported as adults do have a higher login success rate in Objects PassTiles for both login attempts as compared to children but they have similar success rates for Image and Words PassTiles. Adults also had a higher degree of correctness in all three password schemes for the first login as compared to children. For the second login of Image and Words PassTiles adults and children had a similar degree of correctness. Adults took significantly less time to login as compared to children for each login attempt in all three password schemes.

H2a Children performed equally well in all three password schemes in terms of login success rate and degree of correctness for both login attempts. They took significantly longer logging in with the Words PassTiles as compared to the other two password schemes. Therefore, this hypothesis is not supported as there is no indication of children performing significantly better in Objects PassTiles.

H2b Adults had a significantly higher login success rate and degree of correctness during the second login attempt for Objects Passtiles as compared to the other two password schemes. They also took significantly longer to log in with Words PassTiles for both login attempts as compared to the other password schemes. Hence, this hypothesis is not supported. However, we can say that adults perform better in Objects PassTiles as compared to the other two password schemes.

H3 The results collected from the interview data for future use of passwords suggests that children prefer graphical passwords to other types of passwords. Hence, this hypothesis is supported.

H4 By comparing the results of adults and children's password preference for future use we found no statistically significant differences between the two groups. Hence, this hypothesis is not supported.

H5a We took the results from the children's interview where they were asked which password scheme they preferred the most. After comparing children's responses, we found that there was no statistical significance between password schemes. This hypothesis is not supported.

H5b We took the results from the adults interview where they were asked which password scheme they preferred the most. We found that there was no statistical significance between password schemes. This hypothesis is not supported.

5.9 Parent Interviews

We interviewed the parents of child participants to find out more about their home environment in which they spend time online. We asked the parents how much time they allowed their children to spend online. The answer to this varied between 30 minutes to two hours per day and one parent even stated that they allowed their children to spend unlimited time online. We also found out that most children were only allowed to access Youtube, email accounts, educational and gaming websites. Most parents either enforced online parental control restrictions using software tools

or monitored the children's browsing history to make sure that they only went on the allowed websites.

Six parents stated that their children did not have any problems with using their current passwords and that they usually managed their passwords on their own by writing them down somewhere. Five parents said that they would help their children reset the password or create a new one for them when they had problems remembering it. Nine parents stated that their children shared their passwords with them so that they could help if their children forgot the password.

When asked how the parents protected their children's online privacy and security, we got a variety of different answers. Some follow their children's online activities by checking the browsing history. The parents also advised their children not to talk to strangers online or give out personal information like name and address. Almost all parents monitored their children's online activity by only allowing them to use their devices where their parents could easily see them. They also restricted their children's access to certain websites such as Facebook and Twitter. Most children used tablets and laptops to access the Internet.

5.10 Summary

The children took longer than adults during both logins for each password scheme. Children were also less successful in correctly entering their passwords in each scheme as compared to adults. For both adults and children, the highest success rate was for Objects PassTiles for both login attempts. Adults performed slightly better than children for Image and Words Passtiles with a higher success rate for both login attempts.

Adults also outperformed children in all three password schemes during the first login. For the second login adults outperformed children for Objects PassTiles but both performed similarly for Image and Words PassTiles indicating that although the children had memorized fewer tiles initially, their memory appeared more stable. However, children took much longer to login as compared to adults.

In general, children had more difficulty than we expected with the schemes. Looking more closely, we see that most had partially correct entries. This may indicate

that shorter passwords might be more manageable (albeit at a decrease in security) for children. Alternatively, a system which accepts entries as correct if they meet a certain threshold may also be conceivable. Both groups did express interest in using PassTiles over their existing schemes in the future, although exact scenarios were not discussed.

On a positive note, we discovered that children showed interest in creating graphical passwords and memorizing them. We found out that children prefer graphical passwords over other kinds of passwords.

Chapter 6

Discussion and Conclusion

The main goal of our research was to determine the differences and similarities between children and adults when it comes to password memorization and authentication. These factors were tested using PassTiles graphical passwords. In this chapter, we interpret our findings and position them within the literature, discuss our recommended adaptations for children, address the main limitations of our studies, and discuss future work.

6.1 Memorization

The content and organization of images influence the ability to remember an image [4]. We explored three different configuration of PassTiles to see how these affected the memorability of the passwords. Two different memorization techniques were used in the three PassTiles schemes. Objects and Words PassTiles were based on recognition [54] whereas Image PassTiles was based on cued recall [54]. The objects and words, once memorized, were shuffled with each login and had to be recognized from among others while logging in. Participants had to search for and recognize distinct items. The background picture in the Image PassTiles provided the user with a static cue as to which tile to select. Users always needed to choose the same tiles and the image helped distinguish the tiles. We noted that cued recall does not work well when the background image is mostly uniform and includes a lot of tiles of the same color. Therefore, it is important to select an image which has a lot of variety in it so that users can distinguish the tiles easily.

Recognition based PassTiles work better when the user is trying to memorize images of different objects rather than words. We, as humans, are able to remember images much more easily than words, and images are recognized at a higher accuracy as compared to words [40]. Studies also show that pictures are recalled better than

words [31] which has led to the term "Pictorial superiority effect" [30]. The better you are able to visualize something, the better you will remember it at a future time. A couple of participants even visualized the words in Words PassTiles as images in order to remember them. In our studies, Objects PassTiles was most successfully memorized by both adults and children, as evidenced by the highest success rates.

Children took their time to memorize their passwords during the creation phase and practised their password several times before they were ready to log in, yet they still faced difficulty with logins. Adults, on the other hand, did not practice much and memorized most of their passwords just by taking the time to look at them carefully and then started logging in. It was up to the participants whether they wanted to practice the passwords or not but it was recommended that they try it at least once to get it memorized more efficiently. Adults are more familiar with the process of learning passwords than children and may have been better able to draw on these past experiences to come up with successful memorization strategies initially.

6.2 Mental Models

By observing the participants, we were able to gain insight into the formation of their mental models while they were interacting with the system. None of the child participants reported any previous experience with using graphical passwords and only 3 adult participants had prior experience with the grid pattern unlock for their Smartphones. A majority of the participants formed correct mental models of the system during the introduction phase of the study where we showed them a snapshot of each password scheme they would be using.

Four child participants were confused during the start of the study. They started clicking on the tiles highlighted in red to practice their password but when they thought they had memorized the password, they did not understand how to login with it. This required intervention from the researcher who told them to click on the Start button in order to enter their password. These children were of a younger age and required help in order to form the correct mental model for using the system. We note that this difficulty was related to navigation of the interface, and not necessarily with the concept of the password scheme. The adults, on the other hand, did not

require any clarification of how to enter their passwords and adapted to the system quickly. After logging in with the first PassTiles password presented to them in the study, none of the participants had any problems understanding the other two schemes.

After each login, there was a pop up message saying whether the login was successful or not so the participants could know if they made a mistake. This feedback was intended to help with the formation of a correct mental model of the system. This feedback was noticed by almost all adult participants but a majority of the child participants ignored it.

6.3 Usability

The original PassTiles interface was adapted to ensure that it was easy to use for the children. In particular, the amount of text was significantly reduced and the language simplified. The interface was pretty straight-forward for all participants and only minor issues in usability were observed during the study. Two child participants had problem finding the start button which, although visible, was located on the top left of the screen. We could highlight the button to give it better visibility. There was a similar issue with the buttons for selecting a picture in Image PassTiles. Three children did not know how to select the picture and had to be told which button to click.

The interface was kept as simple as possible to make it easy to learn. The children did not show any signs of confusion while using the system and were able to perform the tasks without any major problems. We can say the same for adults who performed all tasks in a good flow and did not encounter any hurdles. The pop up messages provided the feedback required by the participants to get an idea about their performance and to advance to the next step if needed. Most adult participants read the pop up message. However it was ignored by almost all child participants who just clicked the 'OK' button to advance to the next task, assuming they had correctly completed the current task.

For younger children it was observed that a touch screen offered better usability

when entering passwords as compared to clicking with a mouse. Some children accidentally clicked the wrong tile and, having realised that, had to click on the clear button while using a mouse. On the other hand, those children who chose to use a touch screen had fewer problems entering passwords and made fewer mistakes. Three of the children who were seven years of age switched to touch input when using a mouse turned out to be too difficult for them. This took place during the memorization phase when participants were training for entering the passwords.

6.4 User Understanding of Security

We asked the participants some questions related to online privacy and security. Most children had no idea what online privacy and security meant. Five children suggested you should not tell your passwords to anyone or give out personal information to strangers. One child suggested having a strong password and keeping it in a safe place. Another child said that we should avoid clicking on ads and should not give our email address to strangers.

Adults had a more diverse set of opinions for online privacy and security. Four stated that we should change our passwords on a regular basis to keep our accounts secure. Four suggested using anti-virus and to avoid downloading stuff from unknown websites. Four adult participants suggested that we should not log into untrusted websites. A couple suggested having a strong password which is difficult to guess. Another participant suggested that we should avoid phishing attacks. One said that websites keep track of you so you should delete your cookies regularly. Three participants said that we should not tell our passwords to anyone and keep them to ourselves. One participant said that we should restrict access to unsafe websites and keep our data backed up on drives. Two participants suggested that we should not have similar passwords.

Adults has a much better understanding of security and, due to more experience, knew steps to protect themselves online. Children were fairly unaware of security practices and may be more vulnerable to attacks.

6.5 Security of PassTiles Scheme

The PassTiles scheme has several advantages and disadvantages in terms of security. One of the major threats to this scheme is its vulnerability to shoulder surfing where an attacker can look at the password and memorize it while the legitimate user is logging into the system. The shuffling for Objects and Words PassTiles may offer weak protection from casual shoulder surfing but it would not protect the users from attacks where cameras are involved. These schemes should not be used where observation is a concern, but could be suitable for lower security accounts that children may have. There has been previous research on the design and evaluation of a graphical method of authentication that is resistant to shoulder-surfing [56], although its suitability for children has not been evaluated.

Social engineering attacks take place when malicious users attempt to trick users into sharing their login credentials, and the attacker uses these credentials to access the system. Words PassTiles happens to be less resistant to social engineering attacks than the other two variants. Objects and Image PassTiles can be difficult to write down accurately but Words PassTiles could be written down more easily. Similarly, it can be difficult to accurately describe the contents of the Objects or Image tiles that make up the password itself. It would be more difficult for a user to give away these PassTiles passwords than a text password or PIN. PassTiles would also be more resistant to phishing attacks as setting up a phishing website would require greater effort and time as compared to text passwords. Attackers would need pre-access to a user's set of images or would need to act as a man-in-the-middle communicating between the real site and the user.

Users require passwords for many different accounts which can lead to insecure coping mechanisms such as writing them down or reusing them. Graphical passwords are more resistant to multiple password interference [13] than text passwords, therefore might discourage such insecure practices.

It would be impractical to carry out dictionary attacks against the PassTiles graphical passwords using currently available dictionary tools. However, it is possible that scheme-specific dictionaries could be devised. For this reason, we recommend system-assigned passwords so that all passwords are equally probable and dictionary

attacks have no advantage. Graphical passwords like PassTiles tend to have a smaller password space as compared to recall based graphical passwords and hence are more vulnerable to brute force attacks [50].

Previous research has shown that user chosen graphical passwords form patterns [12]. The passwords for the three PassTiles schemes in our studies were selected by the system and hence are less vulnerable to the formation of patterns as the system selects the password for the user randomly. They are also less vulnerable to guessing attacks as the user has no personal preferences of selecting certain Objects or Words that would hold more meaning to them. Therefore, if an attacker attempts to guess the password based on the legitimate user's preferences they would be unsuccessful.

Although not vulnerable to key-logging, PassTiles could be vulnerable to other types of spyware. For example, mouse logging spyware might be an effective tool for breaking the PassTiles password if screen recording and mouse clicks are captured.

6.6 Comparison with earlier studies

In previous research on PassTiles [46] [49], recognition based passwords like Objects PassTiles have been found to be more memorable than free recall conditions like Blank PassTiles where the entire grid is blank. In their studies, it took longer for the participants to login with Objects PassTiles as compared to Image PassTiles which is in line with our study for both adults and children. Our other recognition scheme, Words PassTiles, took the longest to login for both adults and children from among our three schemes.

The higher login times in the two recognition conditions stem from differences in the retrieval processes. Recognition memory involves making a binary decision for each image while traversing the entire image set [46]. This process can be very slow and shuffling the images means that no spacial cues can be used. In contrast, cued recall passwords like Image PassTiles rely on the background image and have fixed locations so the user is able to locate the password faster. Recognition based passwords offer good memorability but the downside is that they take longer to login as compared to cued recall passwords.

6.7 Suggested Adaptations for Children

During the interview, we asked the children what we could do to make the password schemes better. Most participants were generally satisfied with the current design of the password schemes, however, there were some interesting suggestions for improvement in terms of usability. Two participants suggested an improvement for the Image PassTiles where the tile size should be larger. They mentioned that having bigger tiles which are four times the size of the current ones used in the study would make the password much easier to remember. If this is implemented then that would leave us with a total of twelve tiles instead of 48 hence greatly reducing the password space from 21 bits to 10 bits. We could compensate slightly by assigning variable length passwords but we would still not approach the original password space.

Another participant suggested having coloured shapes instead of using Objects to make it easier to remember. There are only a limited number of easily identifiable shapes like circle, square, triangle so this might not be a feasible idea. Having different colours for the same shape in two different tiles could cause confusion for the user but this could be explored. Four participants asked for an improvement in the interface where once a tile is clicked, it should be highlighted so they do not get confused about clicking it again. This would leave the password more vulnerable to shoulder surfing. One way to protect the users against shoulder surfing is to have a toggle button implemented in the system which could turn off the highlighting if the users felt at risk.

A participant suggested adding different background colours to the Objects and Words PassTiles to make them easier to remember. This is a good idea as the user would then be able to associate the item in the tile with the background colour and come up with new ways of memorizing the password although this could increase risks of shoulder surfing. Two participants suggested using more difficult words for Words PassTiles. This idea may be feasible for older children as they would have more unique words as their password but it would present a problem for younger children who might not be able to understand what those words mean. Another participant suggested having the option to choose a picture of their own choice for Image PassTiles instead of having a preselected list of images. This would have no

consequences in terms of security and can be a viable option. The user could also select an image which does not have much variation in terms of colour and objects in it and hence make the system-assigned password very hard to memorize.

6.8 Limitations

In our studies, we asked participants to memorize three graphical passwords consecutively. This might have put a high memory load on the participants as having to remember multiple graphical passwords could be challenging. We noticed a decline in success rates during the second login as the participants recalled all three passwords. In a real life setting, users would rarely create and recall three passwords in such a short time frame. However, the use of a balanced presentation order ensured that all three schemes were treated similarly so differences in results should be due to differences between schemes.

We conducted the studies on an interface where we generated the passwords for the participants and these were not linked to any particular website. We wanted to keep the process as simple as possible for the children and avoid causing any confusion, but this affected the realism of the tasks. We could consider using a website to host the graphical password schemes in future studies for more ecologically valid results.

For our studies, we did a single session with each of our participants to gather all the data and observe the login process. Due to the limited availability of children and their parents, we were unable to schedule follow up studies in which we could have them log into the system with their previously created passwords. We would have preferred to hold this session several days after the participants had created their passwords in order to see how accurately they can remember it in the long term.

If we were to run this study again, we would change the methodology by having the participants learn one PassTiles password at a time. We would then ask the participant to re-enter this password after a few hours to see how much they can recall. This could only be possible if the system was accessible to the participants from home, however, one downside would be that we would not be able to monitor the participants' actions. After the participant is done logging in with one scheme we would then present them with the next one and have them learn the password from

the new scheme, potentially interweaving the sessions as done by Everitt et al. [22]. In our current study, the time gap before the second login is a maximum of 20 minutes during which we conduct the interview.

6.9 Recommendations

Based on our experiences and observations, we make the following recommendations. R1 and R4 apply to both children and adults, while R2 and R3 are targeted more specifically for children's authentication. While we believe that these extensions and applications of our work would be beneficial, these have not yet been tested. Further exploration is required to determine their effectiveness.

R1: Objects PassTiles should be available for low-to-medium security accounts

As Objects PassTiles was the most favoured by participants of both age groups, we would like to recommend that low-to-medium security websites have an option for users to select Objects PassTiles as their password scheme. This would not only satisfy the users in terms of usability but also provide more variability in users' passwords by reducing the amount of password re-use with other accounts. In this way, a compromise to one of the user's accounts would not also compromise the other. This is particularly true if system-assigned Objects PassTiles are used.

R2: Facilitate memorization through learning and training features

We would also like to encourage the creation of stories during the memorization process of both Objects and Words PassTiles by linking together the words or objects that make up the password. We observed several children intuitively using this strategy and believe that incorporating it into the user interface would be helpful. We would recommend incorporating learning/training features to facilitate memorization within the password creation process. Training features that provide an interactive environment for children might prove to be more successful [1], therefore, we would recommend including positive feedback from the system as encouragement. It could be in the form of a gift that the children would have to click to open and see what is inside.

R3: Adapt interface to be age-appropriate for children

We observed age-related differences in how children memorized their passwords and interacted with the systems. As with earlier research, our work indicates that we need different computer interfaces for children throughout the stages of development [6]. This could be in the form of colourful words from age appropriate curriculum or from popular storybooks used in Words PassTiles and familiar objects such as animals and toys in Objects PassTiles for younger children. To help with their interaction with graphical passwords, we recommend using touch screen input instead of mouse input as children tend to accidentally drag and double-click [6] often which could lead to false input.

R4: Combine schemes to improve memorability

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

6.10 Future Work

The literature on user authentication for children is sparse and several related research directions could be explored. For future work, we could compare different types of graphical passwords for children. This would determine which type of graphical passwords are most suitable from a bigger variety. We could also compare the performance of adults and children among other types of passwords like text based passwords and PINs along with graphical passwords. This would help with determining whether graphical passwords are indeed better than other types of passwords in terms of security, usability and memorability.

We could also have children brainstorm their own ideas of a new graphical password that they would like to use in participatory design sessions. We could also hold a similar session with adults. Comparing these ideas would give good insight about each group's preferences. It would help us in determining the common ideas that

adults and children have for usable and secure graphical passwords and provide us with a strong base for implementing new ones suitable for both age groups.

Distinctively coloured backgrounds should be included with Objects and Words PassTiles. Several participants asked for this feature and we believe that the usability advantages would outweigh the slightly increased risk of shoulder-surfing. The colours would help with both the memorization process by giving an extra feature to associate with the tile and with recognition of the tiles while logging on since colour can facilitate visual search.

Our studies were conducted in quiet places either a lab or library. For future work we could consider monitoring the performance in a public place such as school for children and workplace for adults in order to see if there is any difference in performance when there are more people around. This would provide us with better results of their performance based on a real environment where threats such as shoulder surfing also exist and users have to take precaution while entering their passwords.

6.11 Conclusion

Ninety-nine percent of Canadian children between the age of 8-15 years are now able to access the Internet [44]. In this thesis, we compare the performances and preferences of adults and children while they use the PassTiles graphical passwords schemes. We use three schemes, Objects, Image and Words PassTiles, and compare them according to both scheme and age group by using the participants' login success rates, degree of correctness, login times and preferences.

We found that PassTiles passwords were preferred among both adults and children as compared to existing types of passwords. Children had problems memorizing words and were better at memorizing images. Adults outperformed children in Objects PassTiles but had similar performance for Image and Words PassTiles. Objects PassTiles was the best scheme overall as it was favoured by both adults and children, was much easier to memorize and had the highest degree of correctness among the three schemes.

We would recommend the Objects PassTiles scheme to be implemented on websites that are regularly visited by children, giving them the option to choose between

their existing password and graphical passwords. Returning to our main research question comparing adults' and children's performance and opinion of graphical password authentication, we conclude that they perform differently but have similar opinions of the schemes. Adults tend to outperform children in the PassTiles password schemes with respect to login success rates, degree of correctness and login times. This research is a starting point towards development of child friendly graphical passwords. Although more research is necessary in this field to determine the best possible outcome for secure and usable graphical passwords for children, the idea seems promising.

Bibliography

[1] Alissa N Antle. Lifelong interactions embodied child computer interaction: why embodiment matters. *interactions*, 16(2):27–30, 2009.

[2] Robert Biddle, Sonia Chiasson, and Paul C Van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)*, 44(4):19, 2012.

[3] Marilyn A Borges, Mary Ann Stepnowsky, and Leland H Holt. Recall and recognition of words and pictures by adults and children. *Bulletin of the Psychonomic Society*, 9(2):113–114, 1977.

[4] Margaret M Bradley, Mark K Greenwald, Margaret C Petry, and Peter J Lang. Remembering pictures: pleasure and arousal in memory. *Journal of experimental psychology: Learning, Memory, and Cognition*, 18(2):379, 1992.

[5] Sacha Brostoff and M Angela Sasse. Are passfaces more usable than passwords? a field trial investigation. In *People and Computers XIVUsability or Else!*, pages 405–424. Springer, 2000.

[6] Amy Bruckman, Alisa Bandlow, and Andrea Forte. Hci for kids, 2002.

[7] Australian Bureau. Household use of information technology, australia, 2012-13. Technical report, Australian Bureau of Statistics, 2013.

[8] Mark Burnett. *Perfect password: Selection, protection, authentication*. Syngress, 2006.

[9] Karthik Channakeshava, Kaigui Bian, Michael S Hsiao, Jung-Min Park, Robert E Crossler, France Bélanger, Payal Aggarwal, and Janine S Hiller. On providing automatic parental consent over information collection from children. In *Security and Management*, pages 196–202, 2008.

[10] Sonia Chiasson, Chris Deschamps, Elizabeth Stobert, Max Hlywa, Bruna Freitas Machado, Alain Forget, Nicholas Wright, Gerry Chan, and Robert Biddle. The mvp web-based authentication framework. In *Financial Cryptography and Data Security*, pages 16–24. Springer, 2012.

[11] Sonia Chiasson, Alain Forget, Robert Biddle, and Paul C van Oorschot. Influencing users towards better passwords: persuasive cued click-points. In *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction-Volume 1*, pages 121–130. British Computer Society, 2008.

[12] Sonia Chiasson, Alain Forget, Robert Biddle, and Paul C van Oorschot. User interface design affects security: Patterns in click-based graphical passwords. *International Journal of Information Security*, 8(6):387–398, 2009.

[13] Sonia Chiasson, Alain Forget, Elizabeth Stobert, Paul C van Oorschot, and Robert Biddle. Multiple password interference in text passwords and click-based graphical passwords. In *Proceedings of the 16th ACM conference on Computer and communications security*, pages 500–511. ACM, 2009.

[14] Sonia Chiasson, Paul C van Oorschot, and Robert Biddle. Graphical password authentication using cued click points. In *Computer Security–ESORICS 2007*, pages 359–374. Springer, 2007.

[15] Brian A Colella. System for secure internet access for children, December 14 2010. US Patent 7,853,535.

[16] Lorrie Faith Cranor and Simson Garfinkel. *Security and usability: designing secure systems that people can use.* " O'Reilly Media, Inc.", 2005.

[17] Yael M Cycowicz, David Friedman, Joan Gay Snodgrass, and Martin Duff. Recognition and source memory for pictures in children and adults. *Neuropsychologia*, 39(3):255–267, 2001.

[18] Antonella De Angeli, Mike Coutts, Lynne Coventry, Graham I Johnson, David Cameron, and Martin H Fischer. Vip: a visual approach to user authentication. In *Proceedings of the working conference on advanced visual interfaces*, pages 316–323. ACM, 2002.

[19] Allison Druin, Elizabeth Foss, Hilary Hutchinson, Evan Golub, and Leshell Hatley. Children's roles using keyword search interfaces at home. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 413–422. ACM, 2010.

[20] Hermann Ebbinghaus. Memory: A contribution to experimental psychology. *Annals of neurosciences*, 20(4):155, 2013.

[21] Mari Ervasti, Minna Isomursu, and Marianne Kinnula. Bringing technology into school: Nfc-enabled school attendance supervision. In *Proceedings of the 8th international conference on mobile and ubiquitous multimedia*, page 4. ACM, 2009.

[22] Katherine M Everitt, Tanya Bragin, James Fogarty, and Tadayoshi Kohno. A comprehensive study of frequency, interference, and training of multiple graphical passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 889–898. ACM, 2009.

[23] Dinei Florêncio and Cormac Herley. Where do security policies come from? In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, page 10. ACM, 2010.

[24] Stephen S Hamilton, Martin C Carlisle, John Hamilton, et al. A global look at authentication. In *Information Assurance and Security Workshop, 2007. IAW'07. IEEE SMC*, pages 1–8. IEEE, 2007.

[25] Ian Jermyn, Alain J Mayer, Fabian Monrose, Michael K Reiter, Aviel D Rubin, et al. The design and analysis of graphical passwords. In *Usenix Security*, 1999.

[26] Carol C Kuhlthau. Inside the search process: Information seeking from the user's perspective. *JASIS*, 42(5):361–371, 1991.

[27] Stephen Madigan. Picture memory. *Imagery, memory and cognition*, pages 65–89, 2014.

[28] Cliff Lampe Maeve Duggan, Amanda Lenhart and Nicole B. Ellison. Concerns about children, social media and technology use. Technical report, PewResearchCenter, 2015.

[29] Takahiko Mendori, Miki Kubouchi, Minoru Okada, and Akihiro Shimizu. Password input interface suitable for primary school children. In *Computers in Education, 2002. Proceedings. International Conference on*, pages 765–766. IEEE, 2002.

[30] Douglas L Nelson, Valerie S Reed, and John R Walling. Pictorial superiority effect. *Journal of Experimental Psychology: Human Learning and Memory*, 2(5):523, 1976.

[31] Allan Paivio, Timothy B Rogers, and Padric C Smythe. Why are pictures easier to recall than words? *Psychonomic Science*, 11(4):137–138, 1968.

[32] Denise C Park. The basic mechanisms accounting for age-related decline in cognitive function. *Cognitive aging: A primer*, 11:3–19, 2000.

[33] Adrian Perrig and R Dhamija. Déjà vu: A user study using images for authentication. In *USENIX Security Symposium*, 2000.

[34] Janet C Read and Russell 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*, pages 288–292. British Computer Society, 2009.

[35] Janet C Read and Brendan Cassidy. Designing textual password systems for children. In *Proceedings of the 11th International Conference on Interaction Design and Children*, pages 200–203. ACM, 2012.

[36] Karen Renaud and Antonella De Angeli. My password is here! an investigation into visuo-spatial authentication mechanisms. *Interacting with computers*, 16(6):1017–1041, 2004.

[37] Jennifer A Rode. Digital parenting: designing children's safety. In *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology*, pages 244–251. British Computer Society, 2009.

[38] Mei Rose, Gregory M Rose, and Jeffrey G Blodgett. The effects of interface design and age on children's information processing of web sites. *Psychology & Marketing*, 26(1):1–21, 2009.

[39] Bruce Schneier. Sensible authentication. *Queue*, 1(10):74, 2004.

[40] Roger N Shepard. Recognition memory for words, sentences, and pictures. *Journal of verbal Learning and verbal Behavior*, 6(1):156–163, 1967.

[41] Yishay Spector and Jacob Ginzberg. Pass-sentencea new approach to computer code. *Computers & Security*, 13(2):145–160, 1994.

[42] Kevan Stannard. Dinopass password generator for kids, 2013.

[43] National Statistics. Internet access - households and individuals, 2013. Technical report, Office for National Statistics, 2013.

[44] Valerie Steeves. Young candadians in a wired world: Life online. Technical report, Media Smarts, 2014.

[45] Elizabeth Stobert and Robert Biddle. Visual end-user security. In *VL/HCC*, pages 233–234, 2012.

[46] Elizabeth Stobert and Robert Biddle. Memory retrieval and graphical passwords. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, page 15. ACM, 2013.

[47] Elizabeth Stobert and Robert Biddle. The password life cycle: user behaviour in managing passwords. In *Proc. SOUPS*, 2014.

[48] Elizabeth Stobert, Sonia Chiasson, and Robert Biddle. User-choice patterns in passtiles graphical passwords. In *Annual Computer Security Applications Conference (ACSAC) 2011*, 2011.

[49] Elizabeth Ann Stobert. *Memorability of assigned random graphical passwords.* PhD thesis, Carleton University Ottawa, 2011.

[50] Xiaoyuan Suo, Ying Zhu, and G Scott Owen. Graphical passwords: A survey. In *Computer security applications conference, 21st annual*, pages 10–pp. IEEE, 2005.

[51] Tetsuji Takada and Hideki Koike. Awase-e: Image-based authentication for mobile phones using users favorite images. In *Human-computer interaction with mobile devices and services*, pages 347–351. Springer, 2003.

[52] Furkan Tari, Ant Ozok, and Stephen H Holden. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *Proceedings of the second symposium on Usable privacy and security*, pages 56–66. ACM, 2006.

[53] Francis Kapo Tse, Zahra Langford, Jennifer Watts-Englert, Catherine McCorkindale, David Russell Vandervort, and Mary Ann Sprague. Alternate game-like multi-level authentication, February 5 2013. US Patent App. 13/759,369.

[54] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. Authentication using graphical passwords: Effects of tolerance and image choice. In *Proceedings of the 2005 symposium on Usable privacy and security*, pages 1–12. ACM, 2005.

[55] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. Passpoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, 63(1):102–127, 2005.

[56] Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, and Jean-Camille Birget. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *Proceedings of the working conference on Advanced visual interfaces*, pages 177–184. ACM, 2006.

[57] Nicholas Wright, Andrew S Patrick, and Robert Biddle. Do you see your password?: applying recognition to textual passwords. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, page 8. ACM, 2012.

[58] Moshe Zviran and William J Haga. Cognitive passwords: The key to easy access control. *Computers & Security*, 9(8):723–736, 1990.

Appendix A

Interview Questions

A.1 Children

1. How old are you? What grade are you in?
2. What kind of passwords do you currently use on your computer/tablet/phone?
3. Do you like using this password? Why? Why not?
4. Which type of password did you like the most? Why?
5. Which one was the most difficult? Why?
6. Would you like to use one of these different passwords instead of your regular one? If so which one?
7. How do you think we could make these passwords better?
8. How often do you use a password in a day? Where do you login with this password?
9. Do you use more than one password? How do you remember them?
10. Which of the passwords do you think is safest? Why?
11. Do you know anything about privacy and security online? What should you do to make sure you are safe?
12. Who taught you to create passwords?
13. What do you do when you forget a password?

A.2 Parents

1. How much time do you allow your child to spend online?
2. Are there any websites that you are aware of that your child uses regularly?
3. Does your child have any problems with passwords?
4. Do you help your child with his/her passwords or do they manage it on their own?
5. What do you do when your child forgets a password and can't log in?
6. Does your child share his/her password with you?
7. What steps do you take to protect your child's online privacy and security?
8. Do you monitor your child when he/she spends time online?
9. What devices does your child usually use?
10. What is your opinion of this research on Password Authentication for kids?

A.3 Adults

1. What kind of passwords do you currently use on your computer/tablet/phone?
2. Do you like using this password? Why? Why not?
3. Which type of password did you like the most? Why?
4. Which one was the most difficult? Why?
5. Would you like to use one of these different passwords instead of your regular one? If so which one?
6. How do you think we could make these passwords better?
7. How often do you use a password in a day? Where do you login with this password?

8. Do you use more than one password? How do you remember them?
9. Which of the passwords do you think is safest? Why?
10. Do you know anything about privacy and security online? What should you do to make sure you are safe?
11. Do you have any problems with passwords?
12. What do you do when you forget a password?

A.4 Demographic questionnaire (Parents and Adults)

1. Age:
   - 18 - 20 Years
   - 21 - 30 Years
   - 31 - 40 Years
   - 41 - 50 Years
   - 50+ Years
2. Gender:
   - Male
   - Female
3. Level of Education:
   - High School Diploma
   - College Diploma
   - Bachelor Degree
   - Master Degree
   - PhD Degree
   - Other

Current Job: