KidzPass: Authenticating Pre-Literate Children

Michaela Stewart[1]
Mhairi Campbell[1]
Karen Renaud[1,2,3]
Suzanne Prior[1]

[1]Abertay University, Dundee, UK
[2]Rhodes University, Grahamstown, South Africa
[3]University of South Africa, South Africa

k.renaud@abertay.ac.uk (Corresponding Author)

KidzPass: Authenticating Pre-Literate Children

Early Stage Research

Michaela Stewart, Mhairi Campbell, Karen Renaud*, Suzanne Prior
Abertay University, Dundee, UK
*k.renaud@abertay.ac.uk

ABSTRACT

Many online services require users to authenticate themselves to prove their identity. Text-based passwords are the most widely-used authentication mechanism. Yet a number of population groups struggle with text-based passwords. One of these groups is made up of children aged 3-5. This is an important sector of society, because many of these children use the Internet at home. This was especially true during the COVID-19 pandemic.

Young children can struggle with text-based passwords due to their emerging literacy and immature development. The majority of children do not learn to read fluently until age seven. At age four or five, they generally do not have the required skills to create, retain and manage alphanumeric passwords. This might well leave young children vulnerable when online or impose unrealistic demands on their care givers who support them in authenticating themselves.

Here, we report on the development and evaluation of two versions of KidzPass, a graphical authentication mechanism that specifically relies on the abilities 3-5 year old children can be expected to possess. We conclude by reporting on lessons learned about designing authentication for this target user group.

KEYWORDS

Children, Authentication, Evaluation

1 INTRODUCTION

The password idea has been around since the beginning of civilisation [18, 27]. In the cyber world, they were initially intended for use by software engineers, but they have now been embraced by society at large. The password is essentially a string of alphanumeric characters and/or special characters. As a shared secret, it confirms the claimed identity of the user in order to permit access to information, resources or services.

With the diffusion of technology into schools, children are now using passwords from a very young age [7]. Passwords, being alphanumeric strings, require their owner to be literate. Where this cannot be assumed, the password becomes problematic. Because children are using passwords before they have the requisite skills, they do not necessarily know how to cope [8] and are likely to struggle to create, retain and manage passwords [34]. They might engage in unwise behaviours such as reusing passwords or writing them down. It is very hard to unlearn a bad habit once it has been established [28], so we should try to prevent this from happening.

We will first provide an overview of the reasons for using an alternative authentication mechanism for very young children in Section 2. We will then explain how we went about creating an alternative authentication mechanism for this target user group in Section 3. Sections 4 and 5 then detail the two versions of KidzPass we trialled. Each section explains how the authentication mechanism was designed and evaluated, and reports on the outcome of our evaluations. Section 6 reflects on our two studies, reviews their limitations, and provides guidelines we have derived based on our experiences during these studies. Section 7 reviews the latest research in this area and situates KidzPass within this space. Section 8 concludes.

2 AUTHENTICATING YOUNG CHILDREN

There are three traditional ways to authenticate computer users: (1) what you *know*, (2) what you *hold*, and (3) what you *are*.

The most widely used form of authentication is the "*what you know*" alphanumeric password, which computer users are told to (1) memorise, and (2) not divulge to anyone else. They also have to be able to enter the password correctly. Let us consider how a young child might struggle to meet these seemingly simple requirements.

Memorising and Entering Passwords: Very young children are mostly not yet literate [19], so might not yet be able to parse words into letters of the alphabet. Moreover, consider that the letter displayed on the keyboard is an upper case letter. The letter produced, when typed, is lower case. The child also gets no feedback to help them to confirm that they have entered the password correctly.

Proceedings of 2020 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop, Iowa, USA,
.

Literacy and Password Retention: Gathercole [22] suggests a link between speech-based memory and literacy levels. Sowell [38] explains that children do not reach adult levels of retention ability until adolescence. Emerging literacy is likely to make the retention of passwords less reliable. We clearly need to moderate our memorial expectations when it comes to very young children.

Keeping Passwords Secret: Young children are not necessarily able to distinguish between people they *can* share their secrets with, and those they should not divulge their passwords to [2].

Passwords Entry: When entering a password, we have to mentally track the character position within the password, and advance the position as each letter is typed. This ability is probably poorly formed in young children, with shorter attention spans. Children also differ in their ability to focus attention on a particular task for a period of time.

Spelling Ability: Children with dyslexia [33] are likely to struggle to enter passwords correctly, because dyslexia makes it difficult to learn to read and spell and the hidden nature of the entered password is likely to exacerbate these difficulties.

Summary: By using passwords, we are likely requiring children to use a mechanism before they are developmentally ready. We ought to consider an alternative until such time as they have developed the requisite skills to use passwords.

The other two authentication categories are what you *hold* (tokens) and what you *are* (biometrics). One cannot expect a young child to keep track of a token at their tender age. Biometric mechanisms exist that could easily cope with children's small fingers, and accommodate their growth. While their use can be justified for severely disabled children [3], there are serious privacy considerations with this age group [12, 17]. Moreover, biometric readers are not yet ubiquitous, while keyboards and touch screens are.

An alternative "what you know" authentication mechanism would be one that relies on knowledge of something other than an alphanumeric string. We need to find something else that children reliably know, which an authentication mechanism can test. While passwords test knowledge of alphanumeric strings, we could feasibly use photos of faces or other images, essentially harnessing a *graphical authentication mechanism.*

Graphical authentication mechanisms generally display one or more "challenge sets" each containing one *target image* and several *distractor images.* They rely on the picture superiority effect to ease authentication [31]. There is reason to believe that these mechanisms are suitable for use by this user group [1, 37].

In the next Section, we explain how we went about designing such a mechanism.

3 DESIGN & EVALUATION CONSIDERATIONS

We are proposing a child-tailored graphical authentication mechanism for this age group. These mechanisms, and their design dimensions [36], have been widely studied but not for this age group. Hence we review some of the pertinent design issues here.

(1) Technological naïvety [15, 24]. Fortunate children have computers in their homes but not all children will have this advantage. Some may never have used a keyboard before. We cannot assume that the uninitiated will use the keyboard proficiently. Moreover, if a child is accustomed to a tablet, a school machine with a mouse might easily flummox them.

Hence, we ought to rely on pointing rather than keyboard entry.

(2) Emerging literacy [19]. Children proceed through a number of stages in progressing towards full literacy. The first is pre-literacy, which is the stage that the majority of children inhabit when they start school. They will immediately start to embark on the process of learning to read and write. Yet Ehri argues that, while most children will reach fluency by age 9, not all will do so. Alphanumeric passwords require a measure of literacy that the majority of school entry children will not have.

Hence, in designing the authentication mechanism, the use of pictures instead of text is indicated.

(3) Ability to retain information long term [22, 38]: Passwords have to be retained for variable periods of time, and undoubtedly require children to remember them. Given the admonition not to write passwords down, this requires long-term memory skills.

Hence, we ought to find a mechanism that relies on something the child already knows, something that is specific to the child (so that other children can not guess it).

(4) Ability to enter password without feedback: Entering a password requires a person to enter the characters one at a time, while maintaining the position within their password in their minds. They have to do this without any visual feedback. Adults learn to do this but young children do not necessarily have these skills yet [11].

Hence, once again, the mechanism should not rely on a child to rely on their still immature sequential memory.

(5) Secret keeping [2, 32]: One of the cardinal rules is for passwords to be kept secret. Yet young children are not necessarily able to keep secrets from their friends. Moreover, for children this admonition is more nuanced than it is for adults — they ought to share their passwords with their teachers and care givers, but not with other children. The ability to do this requires a maturity which young children are likely not to have attained. Zhang-Kennedy *et al.* [41] discovered, in their

study with children, that they did not understand the need to keep their passwords secret, confirming this difficulty.

This, once again, reinforces the need to use something that cannot easily be described to another child — a picture is harder to describe than it is to tell someone a textual password.

(6) Security Considerations: The obvious criticisms of these kinds of mechanisms include the fact that their dictionaries are not as extensive as an alphanumeric alphabet, that it is difficult to store target and distractor images securely (i.e. hashed) and that shoulder surfing is a real risk.

These are all valid concerns, but if we consider the child's context of use, they become less of a deal breaker. In the first place, the kind of password a 4-5 year old is able to manage is likely to be very weak, and a graphical password can easily provide a better level of security. Moreover, it has been shown that adults and children tend to prefer graphical authentication mechanisms [4], which seem to be particularly suitable for use in low-risk systems where the mechanism protects information of little value.

(7) Ethical Considerations: Participants in this study were recruited via our university's contacts, from a local nursery and a community organisation. Parents were approached in advance and provided with consent form informing them about the rationale behind the study and what the process would be. Parents were told that no identifiable information would be stored and no photographs would be taken without their consent. When the children met with the researchers, either a parent/guardian or staff member from the nursery was present. The children were informed about the rationale of the study and given an overview of how KidzPass worked. Large sheets with images were created for this. The researcher explained that there was no correct answer when carrying out the tasks, and that if they wanted to stop at any time, they could. Data sharing information was not given to the children due to their youth.

In Conclusion: Table 1 summarises this discussion, and lays out the implications. Based on this analysis, what we propose is to identify a password alternative, one that relies on recognition of images, exploiting the picture superiority effect [31]. By so doing, the alternative will rely on skills that children aged 4-5 can be expected to have. Moreover, it limits the possibility for children to tell other children their authentication secret. Finally, the children should interact with the mechanism on a Tablet to minimise the impact of their technological naïvety.

Table 1: Summary of Discussion and Implications

Consideration	Design Implication
Technological naivety	Use a Tablet to Simplify Interaction [4]
Emerging literacy	Do not require reading ability. Use images instead of passwords [29]
Ability to retain information long term	Use something the child already knows and does not have to memorise. Rely on recognition rather than recall [35].
Ability to enter password without feedback	Do not require the child to engage with obfuscated password entry. Allow them to identify their secrets rather than generating them [4, 29]
Limited Secret Keeping Ability [41]	We should make it more challenging for the child to tell other children their secret. An image, especially a face, is harder to describe than it is to tell someone a simple password [9]. The other alternative is to allow the child to provide a simple drawn image, which they are likely to remember very easily.

4 STUDY 1: USING FAMILIAR FACES

We will call this child-friendly graphical authentication mechanism "KidzPass". We now consider the design dimensions of KidzPass.

Identification. Because very young children are pre-literate they cannot be expected to enter an email address to identify themselves. Hence, we provide them with a picture they can identify with. We used a clip art type image of an animal, which the child could choose themselves.

Authentication. We need to decide on a child-specific target image type,and decide how these will be assigned to each child. We also have to decide on how the distractor images will be chosen, and how many images the challenge set will hold.

Image Type & Choice. The first decisions to make to maximise the effectiveness of this alternative are: (1) the kind of image to use, and (2) where to source the images from.

(1) — Image Type. Some graphical authentication mechanisms have used abstract images [16], faces[1], Mikons [37], or pictures of objects [13]. Of these, faces are naturally memorable with face recognition being mastered at a very young age [5, 14].

[1] passfaces.com

(2) — Image Choice. One of the first graphical mechanisms, Passfaces [39], issues faces. We could allow children to choose their own faces but people were extremely predictable in their choices [20]. Alternatively we could use faces that the children are already familiar with [39] which would enhance memorability. We thus decided to ask parents who agreed that their children could participate in our study to provide a photo of an adult who is familiar to the child, but who does not fetch them from school. This would maximise memorability for the child and minimise the chances that other children would guess which face 'belonged' to other children.

Distractor Images. One of the strongest guidelines for these kinds of mechanisms lies in the choice of distractor images, ensuring that they are not too similar to the child's own target image [36]. Given that all the images would be of faces, we thus had to eliminate known faces from the distractor images, to reduce confusion. Some of the children in our study were related to each other or spent time at each other's homes. We thus used [25] to generate non-existent yet very real looking faces to use as distractor images. Hence, the child's target image would be surrounded by faces they could not possibly know.

Size of Challenge Set. The guidelines for adults warn against a challenge set with too many images [36], and this will be even more of an issue for child-specific images. On the other hand, a challenge set of only 6 images, as suggested by [30], would make it far too easy for another child to subvert the access control mechanism. However, we could offer successive small challenge sets, which would not be difficult for the child to swipe through to find "their" face. This maximises both strength and usability.

Design Summary. KidzPass users will choose one animal image which they will then use to identify themselves to the system. To authenticate, they will swipe through 6 challenge sets populated with faces until they identify "their" familiar face.

Figure 1 provides an overview of the KidzPass access control process, with Figures 2 and 3 showing what the interface looked like.

4.1 Evaluation

We wanted to evaluate the usability of KidzPass i.e. its efficacy, efficiency and satisfaction [23] for the target audience. As such, we plan to answer the following research questions:

(1) ***Efficacy:*** Are children able to register and log in using KidzPass?
(2) ***Efficiency:*** How long do they take to log in?
(3) ***Satisfaction:*** How do they feel about KidzPass?

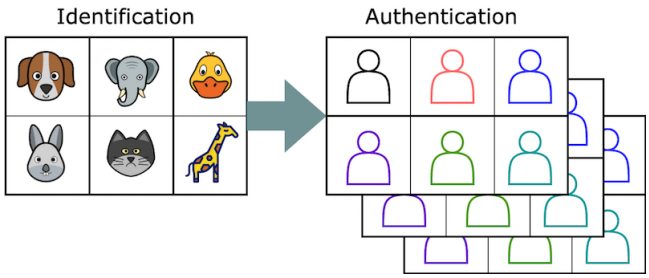

Figure 1: KidzPass Identification & Authentication

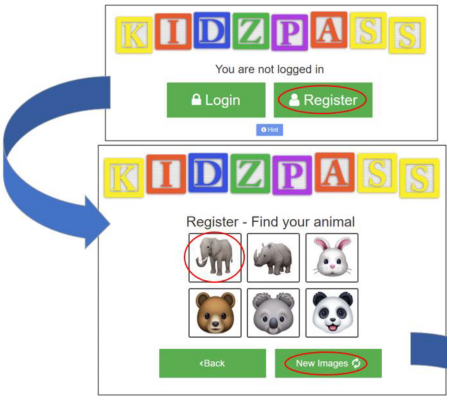

Figure 2: Choosing an Identification Image

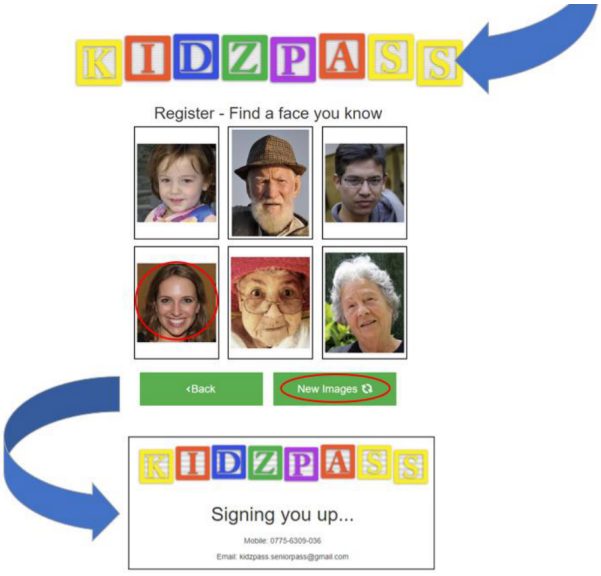

Figure 3: Finding their familiar face

To measure *efficacy*, we recorded the number of successful and failed logins. To measure *efficiency*, the system recorded how long it took the child to log into the system. To measure *satisfaction*, we could not use the traditional SUS scale,

because of the youth of our participants, so we asked the children some questions to gauge their satisfaction with the system after both sessions:

(1) *What did you like about KidzPass?*
(2) *What did you not like about KidzPass?*
(3) *Was it easier or harder to remember a picture instead of a word?*

Once they had logged in, the child could play a game of their choice (Figure 4).

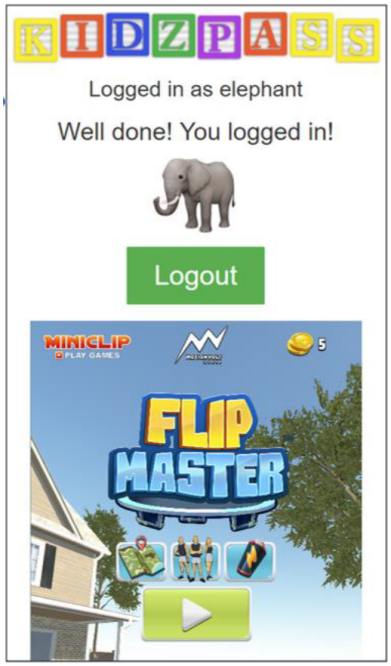

Figure 4: The incentive: a child-friendly game

Recruitment. The evaluation took place in a local nursery and on the University campus. The nursery consented to this project, sent out consent forms and information letters to all parents during February 2019. Parents were provided with an overview of the project and contact details in case they wished to ask further questions. Parents were asked to provide a photograph of a familiar adult for use by KidzPass. These photographs were sent as digital copies to an email account in the project's name, which only the researcher had access to.

We were only able to recruit eight children (six male, two female) to participate in this study. In retrospect, this might have been due to the effort we required from the parents in providing us with an image. The instructions we sent for taking the photo might well have been too complex, and created too much friction, which probably put them off consenting.

Evaluation Stages. The evaluation took place as depicted in Figure 5:

First Session:
During the first session, the child:

(1) *Registered*: by choosing an identification image (this replaces the commonly-used email address). They were then shown how to choose "their" familiar face.
(2) *Logged in*: and played a child-appropriate game.
(3) *Expressed their opinions:* of KidzPass when asked the questions detailed in the previous section. Children were given stickers as a reward for taking part in the study.

Second Session:
A week later, the child:

(1) *Logged in*: with their chosen animal identification image and "their" familiar face. They played a child-appropriate game.
(2) *Expressed their opinions:* of KidzPass when asked the questions detailed in the previous section. Children were given stickers as a reward for taking part in the study.

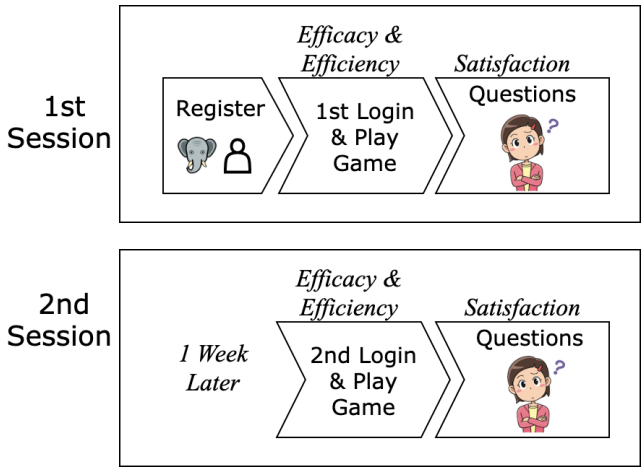

Figure 5: KidzPass Evaluation Phases

Figures 6 and 7 show a child participating in the KidzPass evaluation. These images are used with parental consent.

4.2 Results

Given that we only had eight participants, we conducted a qualitative analysis.

4.2.1 ***Effectiveness***. Table 2 shows the number of errors made by the children at each stage of the evaluation (Registration, 1st Login, 2nd Login). One child selected the wrong

Figure 6: A four year old child choosing his identifier in KidzPass

Figure 7: A four year old child choosing 'his' face using Kidzpass

face during registration, another selected the wrong face at the first login. One chose the wrong identification image at the 2nd login. One child pressed the Registration rather than the Login button, which is understandable since none of these children could read. On reflection, this was a suboptimal design choice. However, all three children recovered from their errors and logged in successfully.

4.2.2 ***Efficiency.*** To report on KidzPass efficiency, we recorded how long it took for the children to register and log in, at both the first and second sessions. Table 3 reports timings for each of the child participants, with a graph depicting the timings in Figure 8. It should be noted that these timings are dependent on the randomisation algorithm so that a longer time could mean that the child had to swipe through a number of challenge sets before seeing "their" picture. However,

Table 2: Number of Errors Made at each Stage (A=Authentication Error; I=Identification Error; B=Button Error)

Child #	Registration	1st Login	2nd Login
1	0	A	0
2	A	0	0
3	0	0	I
4	0	0	B
5	0	0	0
6	0	0	0
7	0	0	0
8	0	0	0

they do give us a sense of how long it would take for a child, on average, to authenticate using KidzPass.

Table 3: Registration and Login Times per Child

#	Registration Time	Login Time (1)	Login Time (2)
1	36 sec	13 sec	54 sec
2	65 sec	91 sec	4 sec
3	169 sec	37 sec	90 sec
4	131 sec	69 sec	124 sec
5	63 sec	30 sec	149 sec
6	66 sec	20 sec	80 sec
7	119 sec	224 sec	130 sec
8	39 sec	9 sec	52 sec

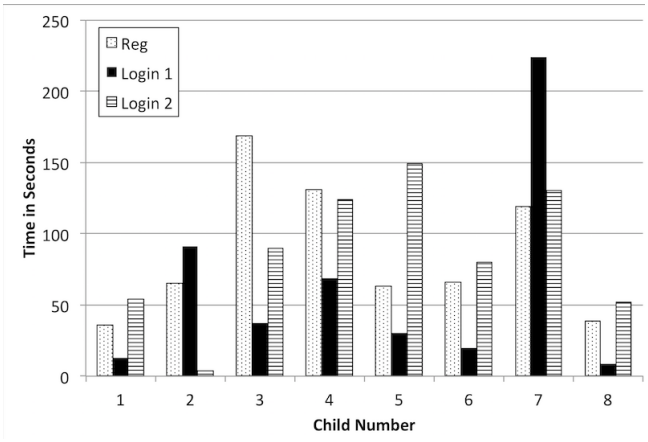

Figure 8: Registration, First and Second Login Times

4.2.3 ***Satisfaction.*** KidzPass requires children to swipe through challenge sets until "their" face appears. It randomly populates the challenge sets. This meant that the children

sometimes had to swipe through multiple challenge sets before they saw "their" face. We observed some frustration with two of the children and this design decision was reconsidered for the next versions of KidzPass.

We asked the children a number of questions after the first session:

(1) *What did you like about KidzPass?* Five of the children immediately said the best part was the game. The other three liked using KidzPass and seeing their relatives' faces on the screen.
(2) *What did you not like about KidzPass?* Seven of the children could not think of anything they disliked but one child said it took too long for "their" face to appear.
(3) *Was it easier or harder to remember a picture instead of a word?* All the children preferred the face image to a word.

We asked the children the same questions after the second session.

(1) *What did you like about KidzPass?* Seven of the children immediately said the best part was the game. One mentioned liking seeing their relatives' face on the screen.
(2) *What did you not like about KidzPass?* Six of the children could not think of anything they disliked but two children said it took too long for "their" face to appear.
(3) *Was it easier or harder to remember a picture instead of a word?* Seven still preferred the face image, but one said he could also remember a word.

4.3 Discussion

At the commencement of this project, the initial aims and objectives were to create a prototype web application system that allowed children to log in using a graphical authentication mechanism. The target user group for the mechanism was children aged 4-5. To assess usability, we measured the following:

(1) ***Efficacy:*** *Are children able to register and log in using KidzPass?* The evaluation, admittedly with only 8 children, demonstrated that they could identify "their" animal image and log in successfully by identifying "their" familiar adult. The children's increased confidence during the second session was particularly noticeable.
(2) ***Efficiency:*** *How long do they take to log in using KidzPass (Doodle)?* In terms of efficiency, the timings are a less than reliable indicator because the login time depends on the randomisation process, which decides when the child's familiar face will appear.
(3) ***Satisfaction:*** *How do they feel about KidzPass?* The children mostly preferred the facial images to text-based passwords. From the qualitative data gathered during the interviews with the children, it is clear that the children prefer graphical passwords over text-based passwords. However, due to the very small sample size and the suboptimal design decisions, it is clear that a follow up study is indicated.

Hence, KidzPass demonstrated effectiveness and satisfaction. It has to be acknowledged that their enthusiasm for the game might have cast a rosy glow over KidzPass itself, but they certainly did not respond negatively when asked for their opinions.

Although a text-based system was not tested in direct comparison, the children had clearly used passwords in other settings and expressed a preference for this graphical authentication mechanism.

5 STUDY 2: DOODLE PASSWORDS

Some design features were retained for the second version. In particular, the identification mechanism (using a picture of an animal) proved popular and memorable. In terms of authentication, we also retained the idea of a child-specific image. Note that the registration button has been moved to the bottom of the interface, requiring the user to scroll down to see it — this prevented the children from pressing it accidentally.

Image Type & Choice. Our previous study's difficulties in recruiting children, and our realisation that this was due to the fact that we were giving their parents too much trouble, made us realise we needed a different kind of image. We thus decided to use the children's own drawn doodles. Doodles have indeed been used by other studies, one with preteens [37] and another recent paper with children slightly older than our target user group [1]. Such images have superior memorability [21, 26] and, we believed, would be a good alternative to familiar faces. The children were provided with a template, as shown in Figure 9, to provide the researcher with two doodles. The revised interface (with reduced text) is shown in Figure 10.

Distractor Images. Whereas our first study used computer generated pictures of *faux* people as distractors, in this study we used pictures drawn by the researcher herself. In this way we could ensure that the distractors were different from the child's own drawn doodles and would not confuse them. A sample of these is provided in Figure 11.

Size of Challenge Set. We used the same size challenge set, since the children had coped well with the six image display and the swiping between different challenge sets to find "their" image.

5.1 Evaluation

Recruitment. Children were recruited from the Rainbows youth group in Broughty Ferry to participate in the study.

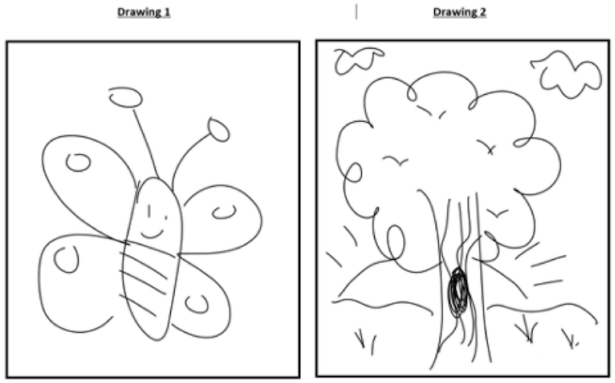

Figure 9: One Child's KidzPass Doodles

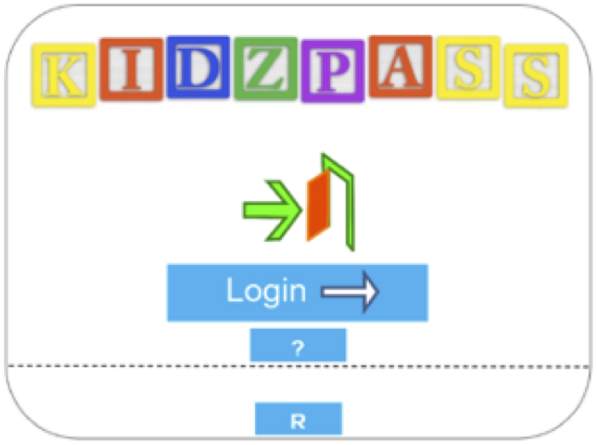

Figure 10: Revised KidzPass Interface

Their parents provided signed consent and the Girl Guide leaders were always present during the initial enrolment (doodle drawing) phase and the authentication phase a week later. Nine children participated, aged 5-6. These participants were generally a year older than the children in the first study, and had had started school.

Qualitative data was also collected through participant observation and interviews which provided a deeper insight into the perceptions of the application. Each participant was given approximately 10 minutes for testing, this was not a time limit however as participants could spend however long they needed with the application. After completing a successful login, each participant was rewarded with an online game and a sticker for taking part.

Evaluation Stages. The evaluation took place in as depicted in Figure 12.

Figure 11: KidzPass Distractor Doodles

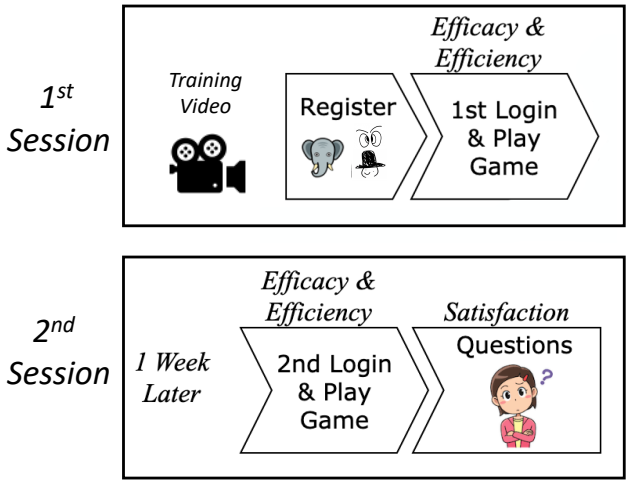

Figure 12: Evaluation Phases

Before the first session, the researcher visited to give the children the opportunity to draw two doodles each. These were uploaded to the system in readiness.

First Session:
The child:

(1) *Watched a Video*: to explain how the system worked.

(2) *Registered*: by choosing an animal identification image.
(3) *Logged in* by identifying their doodles: and played a child-appropriate game.

Second Session:
A week later, the child did the following:

(1) *Logged in*: with their chosen animal identification image and identified "their" two doodles and then played a child-appropriate game.
(2) *Expressed their opinions:* of KidzPass. Children were given stickers as a reward for taking part in the study.

The only slight difference from the first study was that we were not able to ask children questions at the end of the first session due to time constraints. Figure 13 shows the two phases of logging into the system.

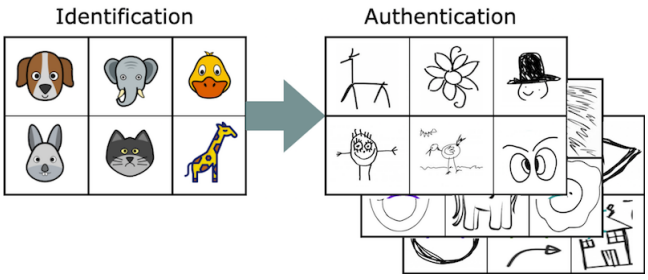

Figure 13: KidzPass Identification & Authentication (Second Study)

5.2 Results

5.2.1 ***Effectiveness.*** The animal identification username images were the most popular feature of the application. This success could be due to popular animal-based films, television shows and books which encourage young children to form a positive relationship with animals.

Two children had to authenticate twice at the 1st login and this happened again to two children at the second login. The failed login attempts were mostly caused by selection inaccuracies and by one participant who struggled to remember their animal image. Child 8's username image was the bee, but they believed that their image was the frog. The frog had featured in the tutorial video as an example, which may be why this participant mistook their image. After realising this, the researcher removed the frog from selection entirely to prevent any further confusion.

5.2.2 ***Efficiency.*** The times taken during the three stages are shown in Table 4. One can observe the general trend of improvement at the second login.

Table 4: Registration and Login Times in Second Study

#	Registration Time	1st Login	2nd Login
1	166s	27s	98s
2	28s	29s	31s
3	73s	34s	28s
4	59s	42s	22s
5	60s	19s	33s
6	75s	29s	20s
7	75s	23s	29s
8	77s	109s	79s
9	119s	63s	20s

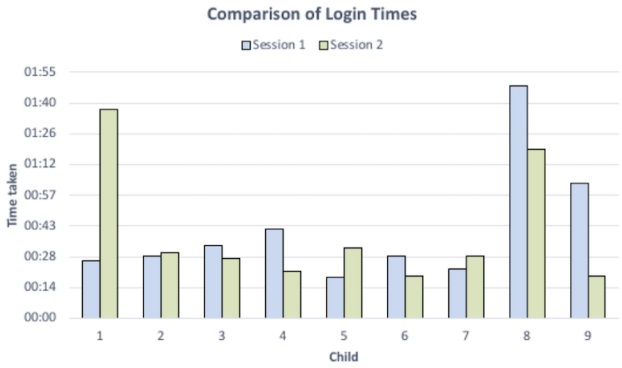

Figure 14: KidzPass Identification & Authentication Times (Second Study)

5.2.3 ***Satisfaction.*** Research was conducted before testing to identify appropriate interview techniques regarding children. Vasquez [40] provide useful guidelines that heavily influenced the interview process. The questions were kept short and simple and the interview sheet was designed to provide a visual component to the interview (Figure 15). Bright colours were used to engage participants and emoticons were included to visually convey the idea behind each question. The questions themselves were mostly open-ended to allow them the freedom to express their responses.

Q1: The children liked the animal identification image (5) and the game (4). Two liked drawing doodles and three liked choosing the image to log in.

Q2: Most of the children said there wasn't anything they didn't like, with one not liking the tutorial video and another not liking clicking on a button.

Q3: Two children said they would have liked a different game to play after they logged in. The others did not make any suggestions about changes.

Q4: Two children said they recognised other images, but these two children did not select those images when logging in.

Figure 15: The questionnaire used to assess satisfaction

Q5: Five children said they could remember their images easily, while 4 were not sure. However, all were indeed able to correctly identify their images when logging in.

Q6: One child said she had found it difficult to identify her images on the screen, while the rest did not have any difficulties.

Q7: One of the children said she preferred using text-based passwords because she used them in school and was familiar with them. The other eight liked the doodle password.

Q8: All the children had fun doing the experiment.

5.3 Discussion

The researcher implemented a short training video which explained how to use the application. One child complained that the tutorial video was too long and some children did seem impatient during the video. To address this, interactivity elements should accompany the video to maintain their interest and enhance the learning experience. Also - the animal image used in the video should not appear in the application itself to avoid confusion.

To assess usability, we measured the following:

(1) ***Efficacy:*** *Are children able to register and log in using KidzPass (Doodle)?* The evaluation, admittedly with only 9 children, demonstrated that they could identify "their" animal image and log in successfully by identifying their own doodles. The children's increased confidence during the second session was particularly noticeable.

(2) ***Efficiency:*** *How long do they take to log in using KidzPass (Doodle)?* The children's times were much improved during the second session as they became more familiar with the application

(3) ***Satisfaction:*** *How do they feel about KidzPass (Doodle)?* Most children agreed preferred to use KidzPass rather than the text-based passwords used in school. The children unanimously agreed that they had fun using the application everyone had something positive to say about KidzPass.

6 FINAL REFLECTION

Based on our two experiments, we now present some guidelines for designing graphical authentication mechanisms for 4-6 year olds.

In designing a graphical authentication mechanism, it is crucial to design with the capabilities of the target users in mind. For young children, we have to accommodate their pre- or emergent literacy and tendency to become frustrated. The particular lessons we learned from our evaluation are listed below.

Use Icons as well as Text: The use of text on the login screen should be avoided. One of the mistakes the children made in the first study was to click on 'Register' instead of on 'Login'. In the second study, the register button was moved to the bottom of the screen so that it could not be pressed accidentally. Moreover, the login button was changed to a simple open door in the second study, to signify entry to the system. On buttons, icons should always be used as well as text, so that pre-literate children are also able to infer the button's purpose.

User Testing is Critical: User testing with the intended user population is the only way to determine if the designed system is suitable. It should be carried out throughout the development process. Testing early with a small sample group of children can highlight many issues that can then be remedied before the final roll out.

Identification Image Choice: The researcher also noted that the animal identification images were very popular. Allowing the children to select their "favourite" animal created a connection between the child and their username image and since most of the children were able to recall their animal image without assistance, this also confirms the superiority of picture memory, even in very young children [31].

Authentication Image Type must be chosen carefully: The image type chosen for the graphical password is key to the success of the application. Using pictures of familiar adults was very successful in the first study as it didn't require the children to memorise a specific image. They immediately recognised their familiar face and were able to associate that face with logging into KidzPass, even when it was surrounded by other faces. The children quickly realised that each picture was different and knew that one was "theirs". The doodles were equally memorable in the second study, proving a reasonable replacement for familiar face images.

Randomisation of Image Choice: The faces shown in the first study's challenge set were randomly chosen. Children could swipe through the sets until "their" face appeared. Some of them became frustrated when they had to swipe through a number of successive challenge sets. Hence, the next version of KidzPass implemented a maximum number of challenge sets to swipe through before the child's doodles appeared. This change worked well.

Incentives Matter: User incentives are important in providing a desire for the young children to want to engage with the system. This applies to the stickers the children were rewarded with after using KidzPass. This good feeling was paired with the success of logging in and the gratification of getting to play the game. This meant the children were excited to use the system in the follow up session and enjoyed the process. The general sense that authentication was not just an adult practice but something they could do independently pleased them. They especially liked the fact that they were securing their very own secret (the game).

Delivery Method Matters: Using a tablet for user testing proved a good choice. There was one incident in the first study where a child accidentally selected an image while attempting to scroll downwards. This was mostly likely due to the learning curve that comes with using a tablet computer and depends on the size of the tablet screen. The researcher found that with a smaller, slower tablet (Nexus 7) there was a higher risk of this happening.

Recruitment: We had some difficulty recruiting children. In the first study, we realised that this was because we were asking parents to do more than sign a consent form. We were asking them to provide us with a photo of someone familiar to the child. We had provided them with complete instructions for what the photo should look like. In retrospect, we created a barrier to participation in very busy parents' lives. For the second version of KidzPass we switched to asking the children themselves to draw images for us. This removed the barrier study 1 imposed. Parents were then happy to permit their children to participate in this case.

Yet, these kinds of studies have stringent ethical requirements and we still found it difficult to recruit children. Many schools in our geographical area receive multiple requests to participate in University studies. This has led them to limit the number of requests they acquiesce to.

Both studies were carried out by undergraduate students, who had strict submission deadlines to meet. A future study would benefit from a more extensive run-in so that a longer period of time is available to support recruitment.

Limitations. The small sample size is a limitation in both studies, in terms of carrying out quantitative analyses. The evaluation was also very time consuming because of the age of the participants. For these initial studies, we wanted to hear their voices and not rush them, but rather give them time to express their opinions. We did not believe it to be feasible to test KidzPass online, because we wanted to see what the children were doing and what they said about the experience.

Even with the small number of participants, these initial studies did deliver a number of valuable insights, which will feed into our subsequent authentication mechanisms targeted for use by young children.

7 RELATED RESEARCH

Read *et al.* [35] and Coggins [10] carried out studies to investigate children's understanding of text passwords. Both studies found that children understood the purpose of passwords and knew how to create strong ones. Read surveyed children aged 6-10 and Coggins surveyed children aged 9-12. These are valuable insights but, because of the speed at which children develop we cannot know whether these findings are valid for 4-5 year old children.

We have argued for the use of an alternative to alphanumeric passwords, until such time as children have developed sufficiently to be able to manage them. We argued against other alternatives such as biometrics and tokens, based on privacy concerns and the tendency of children to lose possessions. We thus proposed turning to a graphical authentication mechanism.

A large number of graphical authentication mechanisms have been formulated and evaluated [6]. Yet few have been targeted specifically at children, to accommodate their needs.

Assal *et al.* [4] did extensive research into the use of the PassTiles graphical password scheme as an alternative authentication method for children. The study investigated three variants of the scheme and provided recommendations for designing more child-friendly authentication methods. Their results were explored through user performance and overall, were largely successful suggesting that both groups in the study, child and adult, preferred graphical passwords to their current text-based passwords. Assal *et al.* did not specify the age of the children who participated in their study.

Renaud [37] tested a graphical authentication mechanism with Mikon images, which pre-adolescents drew themselves. The images were very memorable (demonstrating effectiveness) but were also rather predictable, which seemed to be a particular problem with pre-adolescent girls having very close friendships and sharing interests, which their drawings reflected.

Mendori *et al.* [29] examined the use of passwords in Japanese primary schools. They highlight that, currently, users must enter their names and passwords using alphanumeric characters on a keyboard to be authenticated. This system is very difficult for Japanese primary school children who have yet to learn the Roman alphabet. Therefore, the project aimed to design a new interface using symbols the children were more familiar with. The system was then altered by changing factors such as the number of icons, frequency and icon selection time. The researchers designed a mouse-based system with the icons appearing on screen arranged randomly to stop passwords being distinguished using the position of icons. Users input passwords using buttons. Three types of interface were tested with different numbers of icons. The paper does not state how many subjects each interface was tested with, or the ages of the subjects. However, the evaluation of the system was based on the number of correct selections and the average input time. The study found that displaying 16 icons and 3 challenge sets was the fastest. It is difficult, based on these results, to assess whether interface 2 was the best interface for the children without hearing the children's voices or their opinions of the mechanism.

Our work extends these efforts into designing a graphical authentication mechanism for pre-literate children. We heard their voices and allowed them to express their opinions of the mechanism.

8 CONCLUSION

We developed an alternative authentication mechanism, specifically designed for use by 4-5 year olds. We carried out a qualitative evaluation of two versions of KidzPass with eight and nine children, respectively. These were very rewarding studies, which both we and the children thoroughly enjoyed.

The results demonstrated that the children enjoyed using KidzPass and the majority were able to log in without making mistakes. Overall, the results of these evaluations were promising and the guidelines we provide for making secure and usable authentication mechanisms for young children should be useful to other researchers.

In terms of future work, KidzPass needs to be tested with a larger group of children to gather some quantitative data to support statistical analysis.

It would also be beneficial to ask parents and teachers what the child has learnt from their experiences with KidzPass, to ascertain whether they have internalised the need to keep their images secret, and whether they can remember and describe their secret images.

Finally, subsequent studies should be carried out to compare the strength of traditional text passwords chosen by children of this age with the strength of picture-based passwords. This would help us to judge whether the pictures, while accommodating the youth of the users, also enhanced or compromised security.

ACKNOWLEDGEMENTS

The authors would like to express their thanks to the children who participated and to their parents, especially in the first study, for taking the time to provide us with the 'familiar face' pictures. We also thank our colleagues at Abertay University for many thoughtful discussions about KidzPass. Finally, we thank the anonymous reviewers for their insightful comments, which we have used to improve the paper.

REFERENCES

[1] Esra Alkhamis, Helen Petrie, and Karen Renaud. 2020. KidsDoodlePass: an Exploratory Study of an Authentication Mechanism for Young Children. In *HAISA*.

[2] Lida Anagnostaki, Michael J Wright, and Athanasia Papathanasiou. 2013. Secrets and disclosures: How young children handle secrets. *The Journal of genetic psychology* 174, 3 (2013), 316–334.

[3] Ong Chin Ann and Lau Bee Theng. 2011. Biometrics based assistive communication tool for children with special needs. In *7th International Conference on Information Technology in Asia*. IEEE, Kuching, Sarawak, Malaysia, 1–6.

[4] Hala Assal, Ahsan Imran, and Sonia Chiasson. 2018. An exploration of graphical password authentication for children. *International Journal of Child-Computer Interaction* 18 (2018), 37–46.

[5] Lisa Feldman Barrett. 2017. *How emotions are made: The secret life of the brain*. Houghton Mifflin, Harcourt, New York.

[6] R. Biddle, S. Chiasson, and P. Van Oorschot. 2012. Graphical Passwords: Learning from 565 the First Twelve Years. *Comput. Surveys* 44, 4 (2012), 1–41. http://doi.acm.org/10.1145/2333112.2333114.

[7] ChildTrends. 2018. Home Computer Access and Internet Use. https://www.childtrends.org/indicators/home-computer Accessed: April 07, 2019.

[8] Yee-Yin Choong, Mary Theofanos, Karen Renaud, and Suzanne Prior. 2019. Case Study – Exploring Children's Password Knowledge and Practices. In *Usable Security (USEC). San Diego, February*.

[9] Soumyadeb Chowdhury, Ron Poet, and Lewis Mackenzie. 2013. Exploring the Guessability of Image Passwords Using Verbal Descriptions. In *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 768–775.

[10] Porter E Coggins III. 2013. Implications of what children know about computer passwords. *Computers in the Schools* 30, 3 (2013), 282–293.

[11] Nelson Cowan, Angela M AuBuchon, Amanda L Gilchrist, Timothy J Ricker, and J Scott Saults. 2011. Age differences in visual working memory capacity: Not based on encoding limitations. *Developmental Science* 14, 5 (2011), 1066–1074.

[12] Alasdair Darroch. 2011. Freedom and biometrics in UK schools. *Biometric Technology Today* 2011, 7 (2011), 5–7.

[13] Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud. 2005. Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies* 63, 1-2 (2005), 128–152.

[14] Michelle de Haan, Mark H Johnson, Daphne Maurer, and David I Perrett. 2001. Recognition of individual faces and average face prototypes by 1-and 3-month-old infants. *Cognitive Development* 16, 2 (2001), 659–678.

[15] Andrea DeBruin-Parecki, Kathryn Perkinson, and Lance Ferderer. 2000. *Helping Your Child Become a Reader.* ERIC, Pueblo, USA.

[16] Rachna Dhamija, Adrian Perrig, et al. 2000. Déjà Vu - A User Study: Using Images for Authentication.. In *USENIX Security Symposium*, Vol. 9. Denver, CO, United States, 4–4.

[17] Pam Dixon. 2017. A Failure to "Do No Harm"–India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the US. *Health and Technology* 7, 4 (2017), 539–567.

[18] Editors of Encyclopaedia Britannica. 2016. Book of Judges. https://www.britannica.com/topic/Book-of-Judges Accessed: April 07, 2019.

[19] Linnea C Ehri. 1995. Phases of development in learning to read words by sight. *Journal of Research in Reading* 18, 2 (1995), 116–125.

[20] Ali Mohamed Eljetlawi. 2010. Graphical password: Existing recognition base graphical password usability. In *INC2010: 6th International Conference on Networked Computing*. IEEE, Korea, 1–5.

[21] Myra A Fernandes, Jeffrey D Wammes, and Melissa E Meade. 2018. The surprisingly powerful influence of drawing on memory. *Current Directions in Psychological Science* 27, 5 (2018), 302–308.

[22] Susan E Gathercole. 1999. Cognitive approaches to the development of short-term memory. *Trends in Cognitive Sciences* 3, 11 (1999), 410–419.

[23] ISO. 2018. Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts. https://www.iso.org/standard/63500.html.

[24] J Johnson, C Chapman, and J Dyer. 2006. Pedagogy and innovation in education with digital technologies. In *Current Developments in Technology-Assisted Education*, A. I. González-tablas, A. Orfila, B. Ramos, and A. Ribagorda (Eds.). FORMATEX, Spain, 135–139.

[25] Tero Karras, Samuli Laine, Miika Aittala, Janne Hellsten, Jaakko Lehtinen, and Timo Aila. 2020. Analyzing and Improving the Image Quality of StyleGAN. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 8110–8119. https://arxiv.org/pdf/1912.04958.pdf.

[26] Günther Knoblich and Wolfgang Prinz. 2001. Recognition of self-generated actions from kinematic displays of drawing. *Journal of Experimental Psychology: Human Perception and Performance* 27, 2 (2001), 456–465.

[27] B Lennon. 2017. The long history, and short future, of the password. http://theconversation.com/the-long-history-and-short-future-of-the-password-76690 Accessed: April 07, 2019.

[28] Joan F Marques. 2007. Unlearning: The Hardest Lesson of All. *Performance Improvement* 46, 1 (2007), 5.

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

[30] Martin Mihajlov and Borka Jerman-Blazic. 2018. Eye Tracking Graphical Passwords. In *Advances in Intelligent Systems and Computing*, P Magnaghi-Delfino and T Norando (Eds.). Springer, 37–44. https://doi.org/10.1007/978-3-319-60585-2_4

[31] Allan Paivio and Kalman Csapo. 1973. Picture superiority in free recall: Imagery or dual coding? *Cognitive Psychology* 5, 2 (1973), 176–206.

[32] Joan Peskin and Vittoria Ardino. 2003. Representing the mental world in children's social behavior: Playing hide-and-seek and keeping a secret. *Social Development* 12, 4 (2003), 496–512.

[33] Carole Peyrin, Marie Lallier, Jean-François Demonet, Cyril Pernet, Monica Baciu, Jean François Le Bas, and Sylviane Valdois. 2012. Neural dissociation of phonological and visual attention span disorders in developmental dyslexia: FMRI evidence from two case reports. *Brain and Language* 120, 3 (2012), 381–394.

[34] Suzanne Prior and Karen Renaud. 2020. Age-Appropriate Password "Best Practice" Ontologies for Early Educators and Parents. *International Journal of Child-Computer Interaction* 23–24 (2020). https://doi.org/10.1016/j.ijcci.2020.100169.

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

[36] Karen Renaud. 2009. Guidelines for designing graphical authentication mechanism interfaces. *IJICS* 3, 1 (2009), 60–85.

[37] Karen Renaud. 2009. Web authentication using Mikon images. In *2009 World Congress on Privacy, Security, Trust and the Management of e-Business*. IEEE, St Johns, Canada, 79–88.

[38] Elizabeth R Sowell, Paul M Thompson, Christiana M Leonard, Suzanne E Welcome, Eric Kan, and Arthur W Toga. 2004. Longitudinal mapping of cortical thickness and brain growth in normal children. *Journal of Neuroscience* 24, 38 (2004), 8223–8231.

[39] Grinal Tuscano, Aakriti Tulasyan, Akshata Shetty, Malvina Rumao, and Aishwarya Shetty. 2015. Graphical password authentication using Pass faces. *International Journal of Engineering Research and Applications* 5, 3 (2015), 60–64.

[40] R Vasquez. 2000. Interviewing Children. Hunter.cuny.edu. Available at: http://www.hunter.cuny.edu/socwork/nrcfcpp/downloads/Interviewing_Children_0508.pdf Accessed 19 April 2020.

[41] Leah Zhang-Kennedy, Christine Mekhail, Yomna Abdelaziz, and Sonia Chiasson. 2016. From nosy little brothers to stranger-danger: Children and parents' perception of mobile threats. In *Proceedings of the The 15th International Conference on Interaction Design and Children*. 388–399.