

# Principles for Designing Authentication Mechanisms for Young Children; Lessons Learned from KidzPass

Karen Renaud<sup>1,4</sup>, Melanie Volkamer<sup>2</sup>, Peter Mayer<sup>2</sup>, Rüdiger Grimm<sup>3</sup>

<sup>1</sup>University of Strathclyde, UK; <sup>2</sup>Karlsruhe Institute of Technology, Germany;

<sup>3</sup>University of Koblenz, Germany; <sup>4</sup>Rhodes University, South Africa,

<sup>4</sup>University of South Africa, South Africa

## Abstract

Young children routinely authenticate themselves with alphanumeric passwords, but are probably not ready to use them, due to their emerging literacy and immaturity. They might adopt insecure coping tactics, which are likely to become entrenched. Because children have a superior pictorial recognition ability, graphical authentication mechanisms are likely to be more suitable mechanisms for this demographic.

We propose and study KidzPass, a configurable graphical authentication framework to tailor these mechanisms for children of different ages. We carried out two empirical investigations with children aged 4-5 and 6-7 using personalised images as secrets (familiar faces and self-drawn doodles). KidzPass proved efficacious and our young participants (ages 4-7) mostly preferred it to text passwords. The personalised images maximise memorability, but are time intensive to obtain. As children mature, it might be possible to replace these with generic images. We thus carried out a final empirical study with older children using generic images (chosen by the researcher). The third study indicated that generic images can indeed be viable if they display particular qualities, which we enumerate.

From our experiences and the research literature, we conclude by providing principles to inform the design and evaluation of age-appropriate authentication mechanisms for young children, both from an ethical and technical perspective.

## 1 Introduction

There are, traditionally, three ways computer users authenticate, based on: (1) what they *know*, (2) what they *hold*, and (3) what they *are*. The preferred form of authentication is the first: a shared secret, essentially a string of alphanumeric and/or special characters [Zimmermann and Gerber, 2020]. 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, and the pandemic forcing children to use the Internet during home schooling, children are now using passwords from a very young age [ChildTrends,

2018]. Password users should: (1) memorise, (2) not divulge, and (3) be able to enter the password correctly. A young child might struggle to meet these requirements, even more so than adults do.

With respect to *memorising the password*, consider that passwords, being alphanumeric strings, require their owner to be literate. Very young children are mostly not yet literate [Ehri, 1995], so might not be able to recognise and name letters of the alphabet. Children do not reach adult levels of retention ability until adolescence [Sowell et al., 2004].

With respect to *keeping the password 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 [Anagnostaki et al., 2013]. This conflict might confuse them.

With respect to *entering the password*, the password owner has to be able to parse words into individual characters. To do so, the child has 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 [Frey and Bosse, 2018]. Moreover, consider that the letter displayed on the keyboard is an upper case letter. The letter produced, when typed, is lower case, and is likely to be displayed in serif format — different from the letters children are taught to write (a vs. *a*). The child also gets no visual feedback to help them to confirm that they have entered the password correctly.

Because children are using passwords before they have the requisite skills, they do not necessarily know how to cope [Choong et al., 2019] and are likely to struggle to create, retain and manage passwords [Prior and Renaud, 2020]. They might engage in insecure behaviours, such as reusing passwords or writing them down [Ratakonda et al., 2019]. It is very hard to unlearn a bad habit once it has been established [Marques, 2007], so it is worth identifying an age appropriate alternative mechanism that is more suitable for children.

Alternatives should rely on knowledge of something other than an alphanumeric string. Graphical authentication mechanisms might well be a viable alternative. These mechanisms rely on the picture superiority effect to enhance memorability [Paivio et al., 1968]. There is reason to believe that they could be suitable for use by young children [Renaud, 2009b, Alkhamis et al., 2020], with evidence that children can remember pictures better than text [Corsini et al., 1969, Brown and Campione, 1972, Filan and Sullivan, 1980].

The contributions of this paper are:

- The KidzPass framework, demonstrating how the mechanism can be configured depending on the age of the target user group (Section 3). We introduce the three research questions (RQ1, RQ2, RQ3), and then detail empirical investigations into:
  - the usability of KidzPass with 4-5 year old children using familiar faces (Section 4), addressing RQ1;
  - the usability of KidzPass with 6-7 year old children using self-drawn doodles (Section 5), addressing RQ2;
  - the memorability of generic images (sight unseen, chosen by the researcher) (Section 6), addressing RQ3.
- Section 7 reflects on the empirical investigations to answer the research questions and draw out lessons learned.
- Section 8 brings everything together to provide principles to inform future research in this space:
  - A set of ethical design principles for age-appropriate graphical authentication schemes, grounded in the UK’s “Age appropriate design standard” published in September 2020 [Information Commissioner’s Office, 2020] (Table 1).
  - A set of technical design principles for age-appropriate graphical authentication design, derived from: (1) guidelines obtained from the research literature (Section 2.3), (2) challenges that emerged from the KidzPass evaluations (Section 7.2), and (3) qualities that contribute towards the memorability of generic images (Section 7.1) in Table 2.

Figure 1 depicts the structure of this paper, including Section 2, which reviews the latest research in this area and enumerates the insights to feed into an alternate authentication mechanism for young children. Section 9 concludes.

## 2 Graphical Authentication Research

Alphanumeric passwords were originally conceived to authenticate technophiles in the mainframe computer era. Today, they are the dominant authentication mechanism across the globe [Herley and van Oorschot, 2012], used by people from all walks of life. Due to this mismatch between designed-for target audience and actual users, people deploy coping skills to offset the human memorial burden imposed by passwords. This

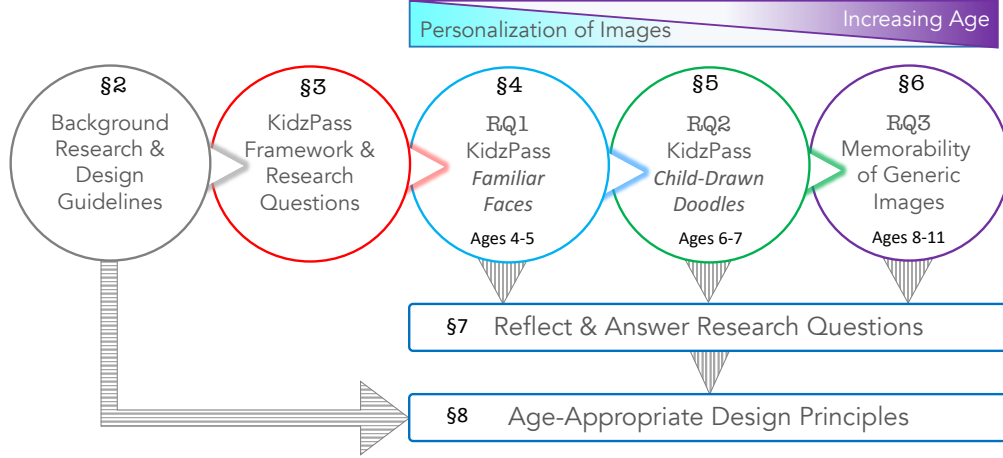


Figure 1: Structure of this paper

weakens the mechanism. One alternative to alphanumeric passwords is the graphical authentication mechanism [Biddle et al., 2012]. These mechanisms rely on the so-called pictorial superiority effect [Nelson et al., 1976]. Paivio’s dual-coding theory [Paivio et al., 1968] posits that visual information is processed and stored differently in the human brain, as compared to random alphanumeric strings. This means that people are more likely to remember pictures, thereby enhancing the memorability of the authentication secret.

## 2.1 Basics

A plethora of graphical authentication mechanisms have been proposed in the research literature [Suo et al., 2005, Mayer et al., 2014, Biddle et al., 2012]. There are three categories of graphical authentication mechanisms, categorized by the kind of memory technique they require [Biddle et al., 2012]: (1) uncued recall-based mechanisms, (2) cued recall-based mechanisms, and (3) recognition-based mechanisms.

(1) When using *uncued recall-based mechanisms*, the user recalls the entire secret and enters it in a predefined blank field (e.g. empty text field for text passwords, a blank canvas for graphical authentication mechanisms). This type is the most cognitively demanding and users experience the greatest memorability issues [Yan et al., 2004, Mulhall, 1915]. Examples of graphical password mechanisms in this category are the traditional Draw-a-Secret mechanism by Jermyn *et al.* [Jermyn et al., 1999], but also more recent proposals [Yang, 2017].

(2) *Cued recall-based* mechanisms improve memorability by providing cues to help users recall the authentication secret. Examples of these mechanisms are the rebus passwords by King [King, 1991], the cued click points mechanism by Chiasson *et al.* [Chiasson et al., 2007] and Weinshall’s cognitive mechanism



[Weinshall, 2006].

(3) *Recognition-based authentication* mechanisms are the third category. These mechanisms generally display one or more “challenge sets” each containing one *target* image and several *distractor* images. The user has to identify ‘their’ target image from each challenge set. Recognition is much less demanding than uncued- or cued-recall [Mulhall, 1915, Tversky, 1973] with fewer authentication failures than passwords [Mayer et al., 2014, Dhamija and Perrig, 2000, Brostoff and Sasse, 2000], and memorability advantages (e.g. [Hlywa et al., 2011, Dhamija and Perrig, 2000]). The ‘secret’ target images can be randomly assigned by the system [Brostoff and Sasse, 2000], chosen by the user [Renaud and Maguire, 2009], provided by the user [Jenkins et al., 2014], or drawn from websites in the user’s browsing history [Chu et al., 2020]. Distractor images have to be chosen with care so that they are not too similar to the target image so as not to interfere with target identification.

## 2.2 Child-Specific Graphical Authentication

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 text passwords. Graphical authentication mechanisms, and their design dimensions [Renaud, 2009a], have been widely studied [Biddle et al., 2012, Shammee et al., 2020], but not for this age group. Before exploring the literature addressing children’s graphical authentication mechanisms, we first address the viability of the other two kinds of authentication from a child perspective: (1) biometrics: ‘something you are’, and (2) ‘something you hold’. The first is unsuitable because it can violate children’s privacy and biometric readers are also not as ubiquitous as keyboards and trackpads/mice. The ‘something you hold’ option would require children to take care of a dongle or other device that they can demonstrate ownership of to authenticate themselves. They may not be mature enough to take care of this, or to prevent older children from appropriating them.

We now review graphical authentication mechanisms that have been evaluated with children. Read *et al.* [Read and Cassidy, 2012] and Coggins [Coggins III, 2013] 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 do not know whether these findings are valid for 4-5 year old children, who are mostly pre-literate.

Assal *et al.* [Assal et al., 2018] did extensive research into the use of the PassTiles graphical password mechanism as an alternative authentication method for children. The study investigated three variants of the mechanism 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.

Mendori *et al.* [Mendori et al., 2002] 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.

The obvious criticisms of graphical authentication mechanisms include the fact that their dictionaries are not as extensive as an alphanumeric alphabet [Biddle et al., 2012], that it is difficult to store target and distractor images securely [Mayer, 2019] and that shoulder surfing is a risk [Darbanian et al., 2015, Li et al., 2005]. These mechanisms are not as strong as text passwords [Renaud et al., 2013]. However, if we consider the child's context of use, this becomes 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 [Assal et al., 2018], which seem to be particularly suitable for use in low-risk systems where the mechanism protects information of little value.

## 2.3 Design & Evaluation Guidelines

An age-appropriate graphical authentication mechanism could be used as an alternative to password authentication for young children. It is likely to more effectively accommodate different levels of literacy and emerging maturity. Some of the pertinent design aspects (extended from [Stewart et al., 2020]) are now provided (Numbered to ease subsequent referral).

**(G1) *Technological naivety*:** Fortunate children have computers in their homes but not all will have this advantage. Some may never have used a keyboard so it cannot be assumed that the children will be able to use the keyboard proficiently. Moreover, if a child is accustomed to a tablet, using a PC with a mouse might easily detract from the authentication task they are trying to complete. Assal suggests using a tablet to simplify interaction [Assal et al., 2018]. **Hence**, we ought to rely on tapping rather than keyboard entry when authenticating young children.

**(G2) *Emerging literacy*:** Children proceed through a number of stages in progressing towards full literacy [Ehri, 1995]. 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. Mendori suggests using images instead of passwords [Mendori et al., 2002]. **Hence**, in designing the alternative authentication mechanism, the use of text should be minimised.

**(G3) *Ability to retain information long term*** [Gathercole, 1999, Sowell et al., 2004]: 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 use images that maximize memorability: something personal to the child or something they provide.

**(G4) *Ability to interact 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 [Cowan et al., 2011]. Being able to recognise images, rather than entering a password is a better option [Mendori et al., 2002, Assal et al., 2018]. **Hence**, once again, the mechanism should not rely on a child to rely on their still immature sequential memory. **Hence**, we should not require memory of sequences of images, only of the images themselves.

**(G5) *Secret keeping*:** 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 [Peskin and Ardino, 2003, Anagnostaki

et al., 2013]. 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 or adults. The ability to make these distinctions requires a maturity which young children are likely not to have attained.

Zhang-Kennedy *et al.* [Zhang-Kennedy et al., 2016] 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 face or drawing is harder to describe than it is to tell someone a textual password [Dunphy et al., 2008, Chowdhury et al., 2013].

**(G6) *Listen to the children:*** Curtin [Curtin, 2001] and Moore *et al.* [Moore et al., 2008] highlight the importance of hearing children’s voices when involving them in research. Curtin admonishes: “*The children need to be given an explanation of the research in words that they can understand and be told with whom the information will be shared. Children also need to be told that they have a right to dissent, that a decision not to participate will be respected, and that they can stop at any time with no consequences.*” (p. 299). Curtin offers a number of recommendations for designing activities to help children to express their opinions. These include: (1) giving them time to settle down in a quiet environment, (2) asking questions while they’re involved in an activity, (3) making sure they understand that there are no right or wrong answers and (4) make it a conversation, not an interrogation. At all times, the researcher should be alert to signs of fatigue, disinterest or a lack of understanding so that the evaluation can be brought to a close.

**(G7) *Limited attention span:*** Children’s ability to focus, especially in terms of visual attention, is poorly formed in the early years, but develops very quickly as they learn to read [Bosse and Valdois, 2009, Murphy-Berman et al., 1986]. This is especially true for children who suffer from a range of neurological difficulties such as attention deficit syndrome [Williams, 2015]. ***Hence,*** children in the youngest age group should not be expected to have a greater visual attention spans than their age suggests.

**(G8) *Visual acuity:*** Studies have shown that there are age-related changes in recognition dwell time [Fioravanti et al., 1995, Duncan et al., 1994, Murphy-Berman et al., 1986] and in saccadic task performance [Munoz et al., 1998]. This means that we cannot overload their visual centres by presenting too much information in the interface all at the same time. ***Hence,*** interfaces should not be too busy or include unnecessary distractions. Moreover, challenge sets, especially for the youngest group, should not include too many images.

### 3 The KidzPass Framework

We propose the use of graphical authentication for children that relies on recognition of images, exploiting the picture superiority effect [Paivio and Csapo, 1973]. This addresses guidelines G1, G3 and G4 above. Moreover, it limits the possibility for children to tell others their authentication secret. However, we also know that children develop rapidly, and learn new skills very fast (G2, G5, G7 & G8). Hence, we suggest a configurable framework which can ensure that the deployed authentication mechanism matches the child's existing stage of development. We shall now describe the different configuration aspects (Gi refers to guidelines in Section 2.3):

**Interface:** G2 requires the use of icons instead of text, especially for children in the 4-5 and 6-7 age groups.

**Identification:** (refer to G2) Because the children in the first two age groups are pre-literate, they cannot be expected to enter an email address to identify themselves. We can thus configure the system to provide a clip-art type image of an animal they can choose to identify with (one that has not been selected by the child). The oldest group, having learnt how to read and write, can use their personal user name.

**Authentication Image Type:** (G3)

*Age 4-5:* Faces are naturally memorable, with face recognition being mastered at a very young age [de Haan et al., 2001, Barrett, 2017]. Moreover Cordon *et al.* [Cordon et al., 2013] find that children remember high and moderate arousal images more accurately than low arousal images, and familiar faces trigger more arousal than unfamiliar ones [Henson et al., 2000]. KidzPass for 4-5 year old children thus uses familiar faces to maximise memorability.

*Age 6-7:* For this group, KidzPass uses the children's own drawn doodles. Doodles have indeed been used by other studies, one with pre-teens [Renaud, 2009b] and another recent paper with children slightly older than this age group [Alkhamis et al., 2020]. Such images have superior memorability due to the action planning memory they invoke when viewed again [Fernandes et al., 2018, Knoblich and Prinz, 2001].

*Age 8-9:* For this group, KidzPass uses generic images. Using generic images enhances scalability for an age group that are mature enough not to require the personalised images. These images ought to be assigned to children, rather than permitting them to choose, to reduce guessability [Cain and Still, 2018].

**Challenge Set Size:** (refer to G7, G8) The guidelines for adults warn against a challenge set with too many images [Renaud, 2009a], and this is even more of an issue for child-specific challenge sets. On the other hand, a challenge set of only 6 images, as suggested by [Mihajlov and Jerman-Blazic, 2018], would make it far too easy for another child to subvert the access control mechanism. However, it is possible to

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. We thus commence with challenge sets of 6 images for the two younger groups, and increase this to 9 images for the oldest group.

**Number of Target Images:** (refer to G3) Young children have a limited working memory capacity so we do not want to overwhelm them. Hence, children aged 4-5 should only have one target image to identify, with the 6-7 age group having two. The 8-9 year olds should be able to remember 4 secret images with ease [Siegler, 2013].

**Distractor Images:** (refer to G8) One of the strongest guidelines for these kinds of mechanisms lies in ensuring that distractor images are not too similar to the child’s own target image [Renaud, 2009a]. For the youngest group, using familiar faces, to eliminate known faces from the distractor images, and to reduce confusion, we recommend using [Karras et al., 2020] 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 of people they could not possibly “know”. For the 6-7 year olds, KidzPass uses doodles drawn by researchers. This ensures that the distractors will be different from those children draw and they will eliminate confusion. For the generic images, visual similarity should be avoided [Hitch et al., 1988] but this age group has much greater ability to distinguish between images given their greater maturity.

#### **Evaluation related guidelines:**

*Device:* (refer to G1) Evaluations should be carried out using a tablet to minimise the impact of their technological naïvety.

*Memorability:* To test whether children are able to recognise their images after enrolling, we have to return to test their memory after a delay. Ebbinghaus [Ebbinghaus, 1885] proposed a forgetting curve, and explained that most forgetting occurs early on in the process and then slows down later on. Other child-related memory retention studies have tested retention after 7 days [Brown and Scott, 1971, Reese, 1975], which we will follow.

*Listening:* (refer to G6) Allow the child to express opinions throughout the evaluation and give them time to speak and express their opinions.

**Finally**, it is essential for any KidzPass evaluation to be carried out ethically. This means that researchers’ institutions’ ethics review boards should approve the study. Figure 2 depicts the framework, showing the configurable aspects depending on the target user group’s age.

The research questions we explore in this investigation are:

**RQ1:** Is KidzPass, using familiar faces, usable for children aged 4-5?


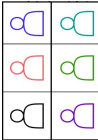
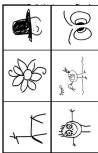

AGE	4-5	6-7	8-9	
IDENTIFICATION				User Name
ACTION TO AUTHENTICATE	Recognize Face	Recognize Two Doodles	Recognize Four Objects	
	Familiar Faces	Hand-Drawn Doodles	Images Of Objects	
IMAGE SOURCED	Provided by Parent	Drawn by Child	Randomly Allocated	
CHALLENGE SET SIZE				
DISTRACTORS	Generated Faces	Doodles Drawn by Researcher	Other Objects	

Figure 2: The Configurable KidzPass Framework

**RQ2:** Is KidzPass, using self drawn doodles, usable for children aged 6-7?

**RQ3:** What qualities should generic images exhibit to make them suitable for use by KidzPass when authenticating children aged 8-9?

## 4 KidzPass for 4-5 year olds: Using Familiar Faces

**Obtaining Authentication Images:** We asked parents to provide a photo of an adult who is familiar to the child, but who does not fetch them from school. This maximised memorability for the child and minimised the chances that other children would guess which face ‘belonged’ to other children.

**Enrolling:** We allowed the children to choose whichever animal picture they liked best to identify themselves. Once a particular image had been chosen, it was removed from the set, so that other children could not choose it.

**Authenticating:** To authenticate, children swiped through challenge sets populated with six faces until they identified “their” familiar face. If they did so successfully, they were able to play a game. If not, they were given as many opportunities as they liked to try again.

**Testing memorability:** A week after enrolling, the researcher returned and asked the children to log into the system again to play the game.

**Ethics:** The University of Abertay’s ethical review board approved the research study. The primary

researcher applied for and obtained an enhanced Disclosure Scotland Check<sup>1</sup>. We obtained signed consent from parents. A teacher was present during all interactions with the children. Children were given a sticker to thank them for their participation.

## 4.1 Methodology

Eight children (six male, two female) participated in this study.

**First Session (Enrolling):** During the first session, the child: (1) *registered*: by choosing an identification image. They were then shown how to choose “their” familiar face by swiping through successive challenge sets; (2) *logged in*: and played a child-appropriate game; (3) *expressed their opinions*: of KidzPass. Children were given stickers as a reward for taking part in the study.

**Second Session (Testing Memorability):** 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. Children were given stickers as a reward for taking part in the study. We evaluated the usability of KidzPass i.e. its efficacy, efficiency and satisfaction [ISO, 2018] for the target audience.

## 4.2 Results

One child selected the wrong face during registration, another selected the wrong face during the first login session. One chose the wrong identification image at the second login. One child pressed the “Registration” rather than the “Login” button, which is understandable since none of these children could read. On reflection, the positioning of the registration button next to the login button was a sub-optimal design choice, and this was corrected before the next evaluation. However, all three children recovered from their errors and logged in successfully. We recorded how long it took for the children to register and log in, at both the first and second sessions. Figure 3 depicts timings for each of the child participants. 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, they do give us a sense of how long it would take for a child, on average, to authenticate using KidzPass. KidzPass requires children to swipe through challenge sets until “their” face appears. It randomly populates the challenge sets. We observed some frustration with two of the children due to their having to swipe through multiple challenge sets before they saw “their” face. KidzPass was subsequently refined so that the number of swipes was limited and did not lead to frustration.

---

<sup>1</sup><https://disclosures.org.uk>



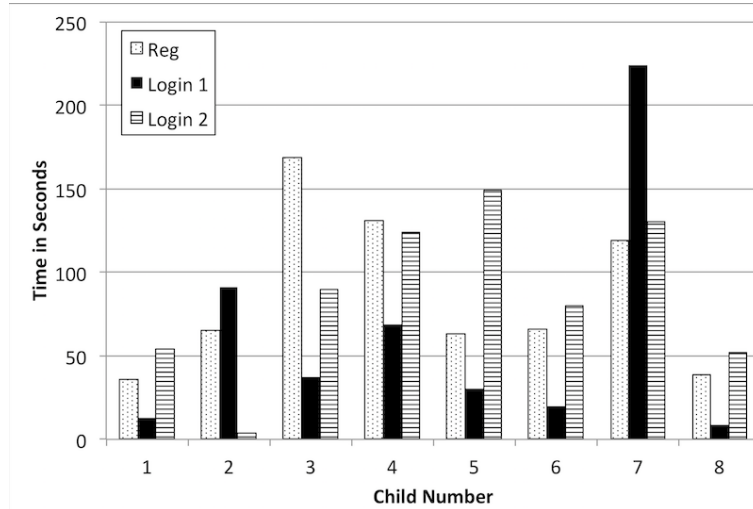


Figure 3: Registration, First and Second Login Times

### 4.3 Discussion

The evaluation, albeit with only 8 children, demonstrated that children aged 4-5 could pick “their” animal image and log in successfully by identifying “their” familiar adult. The children’s increased confidence during the second session was particularly noticeable. In terms of efficiency, the timings are an unreliable indicator because the login time depends on the randomisation process, which decides when the child’s familiar face will appear. From the qualitative data gathered during the interviews with the children, it is clear that the children preferred KidzPass to text-based passwords [Stewart et al., 2020].

In conclusion, KidzPass for 4-5 year olds demonstrated effectiveness and satisfaction. It has to be acknowledged that their enthusiasm for the game is likely to have cast a rosy glow over KidzPass itself, but the children 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 contexts and expressed a preference for KidzPass.

## 5 KidzPass for 6-7 year olds: Using Self-Drawn Doodle Images

**Obtaining Authentication Images:** The children were provided with a template so that they could provide the researcher with two doodles (Figure 4).

**Enrolling:** We allowed the children to choose whichever animal picture they liked best to identify themselves. Once a particular image had been chosen, it was removed from the set, so that other children could not choose it.

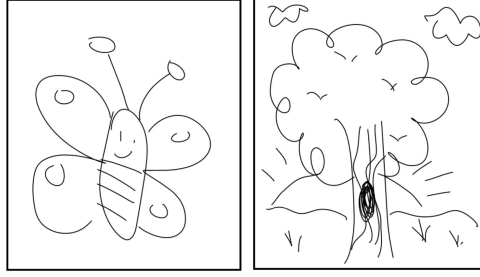


Figure 4: One Child’s KidzPass Doodles

**Authenticating:** To authenticate, children swiped through challenge sets populated with six doodles until they identified both of “their” own drawn doodles. If they did so successfully, they were able to play a game. If not, they were given as many opportunities as they liked to try again.

**Testing memorability:** A week after enrolling, the researcher returned and asked the children to log into the system again to play the game.

**Ethics:** The same procedure was followed as for the previous KidzPass evaluation.

## 5.1 Methodology

The ethical approval process was identical to that of KidzPass for 4-5 year old children. Nine children participated, aged 5-6. These participants were generally a year older than the children in the first study, and had started school.

**First Session (Enrolling):** 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 (Testing Memorability):** A week later, the child: (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.

## 5.2 Results

The animal identification images were the most popular feature of the application, which 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 first 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 identifier. Child 8’s username image was the bee, but she believed that her image was the frog. The frog had featured in the tutorial video as an example, which may be why this participant mistook her image. After realising this, the researcher removed the frog from selection to prevent any further confusion. The times taken during the three stages are shown in Figure 5. Once again, these timings are dependent on the randomness of the challenge sets generated by the algorithm.

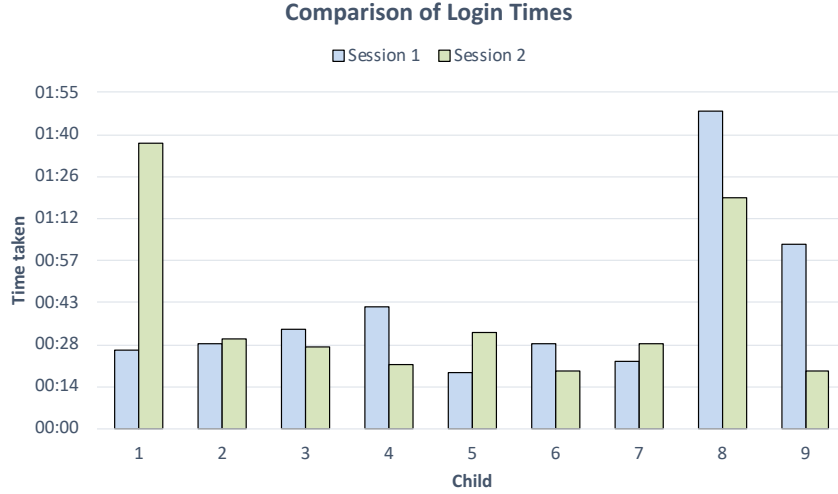


Figure 5: KidzPass Identification & Authentication Times (Second Study)

### 5.3 Discussion

The evaluation, admittedly with only 9 children, confirmed that children aged 6-7 can easily identify “their” animal image and log in successfully by identifying their own hand drawn doodles. The children’s increased confidence during the second session was, again, noticeable. The children’s authentication times improved during the second session as they became more familiar with the application. Most preferred KidzPass to text-based passwords. The children unanimously agreed that they had fun using the application and everyone had something positive to say about KidzPass.

## 6 KidzPass for 8-9 year olds: Identifying Required Qualities of Generic Images

The images we used for KidzPass for the younger children have proven efficacy in the authentication context [Brostoff and Sasse, 2000, Stewart et al., 2020]. KidzPass for 8-9 year olds aims to use generic images to improve scalability, benefiting from the greater maturity of the children. Before we can evaluate

such a mechanism with 8-9 year old children, we need to determine what qualities such generic images should display to be optimal for use in this context. The main quality is memorability, so we carried out an initial study to assess memorability with children aged between 8 and 10 years of age.

**Obtaining the Images:** We used four grids of nine images: (1) nine different animals, (2) nine different cars, (3) nine different ships, and (4) nine different buildings (see Figure 6 for the grids). We used challenge sets with nine instead of six images due to the children's greater maturity, with four images needing to be remembered. We showed the images to the children's teacher to test their suitability in terms of understandability, and she considered them to be appropriate. The four grids are shown in Figure 6.

**First Exposure to Target Images:** The teacher, having welcomed everyone, started the lecture with our memory game. The children were asked to focus on the digital board for a minute. They were told not to speak during this minute and told that they would get more information at the end of the lesson. Note that the need to remember the images was not mentioned when the images were initially displayed. The teacher then displayed one animal, one car, one ship, and one building, each for about 5 seconds, on the digital board. The teacher did not comment on the images and the children simply observed them. All children saw the same images. Note that we did not tell the children that they were participating in a study. For them, it was a memory game. Afterwards, the lesson continued as originally planned.

**Memorability Test:** The immediate memorability was tested using printed grids. Before the lecture, the teacher prepared four one-page grids of images, with images randomly ordered within the grids. At the end of the lesson, the teacher told the children that they would now return to the images they had seen at the beginning of the lecture. They received four pages containing images and were instructed to mark the image in the grid that they had seen before. They were asked not to talk to each other during the task, but rather to wait until everyone had completed the task. They brought their pages to the teacher when they had completed the task. Note that the grids were distributed in such a way that children sitting next to each other got differently ordered grids (just to make sure that it was not easy to see which image others were marking). The delay between showing the images and indicating the correct image within the grids was one hour and 15 minutes. This was sufficient time for forgetting to occur [Ebbinghaus, 1885].

**Memorability Test After 7 Days:** A week later, printed grids were distributed and the children were asked to mark the image they remembered from the previous week. The children received information about the use of these kinds of images in authentication i.e., that such an approach could be used in future to log in to their computers instead of passwords. The teacher explained that, in this case, every child would get a different set of images to remember.

**Ethics:** The 'study' was conducted by their teacher during an informatics lecture. No personal data was collected from or about the children. Their performance and behaviour during the 'study' was not



Figure 6: The four grids used in Study 3.

graded. As such, we did not need to secure ethical approval nor did we have to get permission from their parents.

## 6.1 Results

In total, 44 children participated. The study was conducted in two classrooms. In one, the children were between eight and nine (21 in total) and in the other, between nine and ten (23 in total). The second memorability test could only be conducted in one class due to the COVID pandemic closing schools. We tested this with an older group too to see whether there were marked improvements in memorability in the older group.

*8-9 years of age:* All children remembered the animal. One child selected the wrong car. The correct building was not selected by two children. The correct ship image was not selected by five children. One child who had issues with two image types, six had issues with one image type. The remaining 14 children correctly identified all images in the grids. For this group, it was not possible to collect data a week later.

*9-10 years of age:* At the end of the lesson, the results were as follows: All children got the animal, the

car, and the ship correct. Three children had issues with the building. A week later, half way through the informatics class, the children once again marked the image within the grids. Again, all remembered the animal, the car, and ship. However, this time, five children had an issue remembering the building. Eighteen children got everything correct a week later.

## 7 Reflection

Our experiences during the evaluation of KidzPass for the two younger age groups were positive. The children were mostly able to authenticate both the first and second time, and seemed to enjoy interacting with the mechanism (and with the game). Hence, research questions 1 and 2 can be answered in the affirmative. Children in the oldest KidzPass group had no issues with the animal and the car; the older group also had no issue remembering the ship. However, both age groups had difficulties with the buildings. We have to explore why these differences occurred so that we can use these images in KidzPass for older children, so that we can answer RQ3.

**Existing Knowledge Base:** Ornstein and Naus [Ornstein and Naus, 1985] argue that children’s existing “knowledge base” influences the acquisition, retention, and retrieval of information. This suggests that we should make sure that children have a sufficient working knowledge of the images such that they are able to label them differently. Bjorklund and Zaken-Greenberg [Bjorklund and Zaken-Greenberg, 1981] argues that children construct taxonomies of images in their minds, so that images belonging to the same category are stored together. This suggests that if they do not know individual labels, they might well assign the category label to the secret image they saw. Then when they see multiple images in the same category, this will lead to errors of identification.

It is possible that children of this age are not yet familiar with the individual names of the complex buildings and so could not uniquely label the “secret” image. It would merely be a building, not a ‘beach house’ or a ‘Venetian building’.

**Ability to Label:** It was indeed realistic to expect these older children to be able to memorise these images, given that recognition memory of images improves with age [Cycowicz et al., 2001]. However, and this is linked to the previous point, Hitch and Halliday [Hitch and Halliday, 1983] suggest the existence of two working memory stores: (i) the articulatory loop, which is involved in subvocal rehearsal, and (ii) the visuo-spatial scratch-pad, involved in imagery. The authors argue that “*older children use the articulatory loop to remember picture names: their performance is sensitive to phonemic similarity of the names and articulatory interference*” (p.325). This is interesting because it suggests that the ease with which labels can be summoned will impact the memorability of images for older children, the group we tested these

images with.

Reese [Reese, 1975] also finds that younger preschoolers relied on visual memory to recognise images, while older preschoolers started to use image labels to reconstruct images, relying on their verbal memory. This confirms, once again, the importance of the child being able to assign a label to a generic image in order to encode and retain it in their memory so that it can be retrieved for recognition tasks. KidzPass for the younger children did not tap into the same kinds of memory as the generic images. The first relied on existing familiarity of faces [Gobbini and Haxby, 2007] while the second relied on action planning memory [Knoblich and Prinz, 2001] which is imprinted as the doodle is drawn. In these cases, ease of labelling becomes less important.

**Distractor Choice:** KidzPass for the younger children used personalised images: familiar faces and doodles — all of the images in the challenge sets came from the same category. In hindsight, this strategy did not *have* to be used for generic images, as we did. It might be that when generic images are used, distractor images should be from completely different categories to avoid the labelling difficulties the children experienced. So, for example, if the child’s target image is a ship, the distractor images could be a building, a toy, a bed, and so on.

**Image Content:** Guidelines for designing graphical authentication includes advice that the image should be a single object with a clear background, so that labelling is simplified [Renaud, 2009a]. The building category demonstrates the importance of this guideline. All the images show multiple buildings. These images do not lend themselves to easy labelling. The animals, on the other hand, were easily labelled. Each image shows an easily identified animal, and children learn animal names at a very early age.

**Finally**, it is important to note that the memory check was facilitated by handing out paper copies of the grids in black and white (due to resource constraints at the school). Thus, it is possible that the images children struggled to remember would have been more easily distinguished from other images if they had been printed in colour, with colour providing an extra cue.

## 7.1 Required Qualities of Generic Images:

In answer to RQ3, we suggest that the generic images used by KidzPass to authenticate over 8 year olds should display the following qualities:

**(Q1) Understandability:** Construct challenge sets from images that are substantively different from each other [Fioravanti et al., 1995, Duncan et al., 1994, Murphy-Berman et al., 1986].

**(Q2) Ease of Labelling:** Ensure that your target user age has the vocabulary to label each image

uniquely. This is by no means a given, even for adults. One of the authors on this paper was unable to identify more than two of the cars depicted in the car set. To gauge the kind of vocabulary a child of any age range can be expected to have, looking at children’s books is a good idea [Zwiers and Morrisette, 2013].

**(Q3) Image Content:** The image itself should depict a single object, or multiple objects of the same type (like the horses in the animal category) on a clear (as opposed to busy) background. For example, the bottom right picture in the building category could be depicting a particular city (which a child of that age is unlikely to be able to identify correctly). It also includes a river and what looks like a church. Consider that a child sees this image and chooses the label “river”. Seeing the grid a week later, he/she could easily think that he/she had previously seen the image directly above that one, which could arguably also be labelled as ‘river’. If they picked out the steeple on one of the other pictures showing a steeple, and then saw the entire grid, they would see two pictures with steeples. Hence, graphical authentication images have to be chosen with great care to avoid confusion.

**(Q4) Use coloured images** so that colour can enhance distinctions between images.

**(Q5) Distractors must be distinct** so that the children do not confuse the target with the distractors - differences in labels and visual appearance will help.

## 7.2 Challenges & Limitations

**(C1) Recruitment Difficulties:** The small sample size is a limitation in both studies, in terms of carrying out quantitative analyses. This was due to difficulties in recruiting participants [Stewart et al., 2020]. In the first study, we realised that this was because we were asking busy parents to provide us with a photo of someone familiar to the child. We had provided them with comprehensive instructions. In retrospect, this created a barrier to participation. For KidzPass for 6-7 year olds, we switched to asking the children themselves to draw images for us. This removed the barrier study 1 imposed. Parents were happy to permit their children to participate.

Even so, these kinds of studies quite rightly have stringent ethical requirements. Every parent has to sign a consent form, and teachers have to be able to allocate some time to this activity, twice (register then test memorability). Schools likely receive multiple requests to participate in University studies. This understandably leads them to limit the number of requests they agree to.

**(C2) Time-Intensive Evaluation:** It is infeasible to carry out initial tests of KidzPass online, because we wanted to observe them as they interacted with the mechanism, and hear what they said about the experience. For these initial studies, we wanted to hear their voices and not rush them, but rather give them time to express their opinions. This was a wise strategy which we advise other researchers to follow.



This made the evaluation more time consuming.

**(C3) *Easing Transition to KidzPass*:** The password is used because those who develop systems know that users are familiar with it. We have argued that the password is unsuitable for authenticating young children. KidzPass undoubtedly has benefits for younger computer users. However, to encourage uptake by developers, we will have to make the transition to KidzPass as painless and inexpensive as possible. This starts with using free software, so that there is no additional monetary outlay. It would also be helpful if KidzPass could be provided as a plug-and-play component, which is a topic for future research.

## 8 Age-Appropriate Authentication Design Principles

In designing a graphical authentication mechanism, it is crucial to design with children’s capabilities in mind, and to do so ethically. We have to accommodate their pre- or emergent literacy and tendencies to become frustrated. Based on our studies, we now present principles to inform the design and evaluation of graphical authentication mechanisms for primary school children. We will present two kinds of design principles: (1) Ethical, and (2) Technical, grounded as shown in Figure 7.

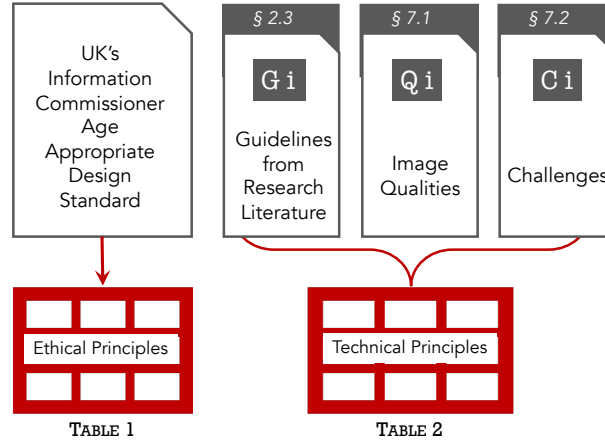


Figure 7: Sources of the Ethical and Technical Principles

### 8.1 Ethical Principles

The UK’s Information Commissioner (ICO) published “Standards of age appropriate design” in September 2020 [Information Commissioner’s Office, 2020]. We used this standard to derive principles to inform the ethical design and evaluation of age-appropriate authentication mechanisms. In Table 1, we contextualise the provided age-appropriate design principles to the graphical authentication context, with the ICO’s principles appearing in the leftmost column. Researchers should seek approval from their institutions’

ethical review boards before commencing any evaluations with children, demonstrating how they align with the ethical principles.

## 8.2 Technical Principles

The technical design principles we present in Table 2 cover the design and evaluation of age appropriate authentication mechanisms developed for research purposes. Using graphical authentication as a password alternative addresses guidelines G4 and G5 (Section 2.3). To date, due to very few empirical evaluations having taken place, we do not yet know how to prioritise these guidelines, nor how to classify them in terms of those that are essential and those that are ‘nice to have’. This is a topic for future research.

## 9 Conclusion & Future Work

We developed KidzPass, a framework for configurable age appropriate graphical authentication mechanisms designed specifically to authenticate young children. We carried out two qualitative evaluations of KidzPass using personalised images. These were very rewarding studies, which both we and the children thoroughly enjoyed. The results of the first two studies demonstrated that the children were able to log in and enjoyed participating.

However, we realised that the mechanism would not scale sufficiently to support wide-ranging deployment, mostly because of the personalised image types we used. We thus carried out a third study, with 44 children, to test the memorability of less personalised images. The results of the third study confirms, once again, the importance of the kinds of images used in these kinds of authentication mechanisms, in terms of maximising memorability and suitability.

Our studies convinced us of the need to provide evidence-based principles for other researchers and practitioners wanting to use an age-appropriate graphical authentication mechanism. We conclude by providing ethical principles in line with the UK’s age-appropriate authentication design standard and technical principles to inform the design and evaluation of these age appropriate graphical authentication mechanisms.

**Future Work:** If we want to deploy KidzPass outside a research environment, we need to address the following:

Table 1: Ethical Principles for designing &amp; evaluating age-appropriate authentication mechanisms (ICO principle in the leftmost column)

Principle	Design	Evaluation
Best interests of the child	Design the mechanism in line with the child’s capabilities.	See Figure 2 and Table 2.
Data protection impact assessment	Develop a Data Protection Impact Assessment (DPIA).	Give children and parents the chance to have a say in how their data is used to help you build trust, and improve your understanding of child-specific needs, concerns and expectations.
Age-appropriate application	User incentives are important in providing a desire for the young children to want to engage with the system. Reward the children for using KidzPass by letting them play a game.	User testing with the intended user population is the only way to determine if the designed system is suitable.
Transparency	The interface of the authentication mechanism should always represent its current internal state to minimise the gulfs of evaluation and execution. For example, prominently display visible cues for children to interpret the state and the interact with to carry out available actions.	Children are capable of assenting to be involved in a research study [Weithorn, 1983]. Obtain this consent. They should be informed that they can stop at any time. Use pseudonyms in writing up the research [Curtin, 2001].
Detrimental use of data	Do not use the child’s data for any other purpose than authentication.	Ensure that parents are informed about the use of their children’s data that is collected for evaluation purposes. Take no photographs without parental consent.
Policies and community standards	Within the EU, ensure that GDPR standards are adhered to. Only collect data that is necessary as part of the authentication and make sure all child-provided data is stored either encrypted or hashed in order to ensure that no sensitive information the child potentially entered can leak in plaintext. If encrypted or hashed storage is not possible, ensure that it is clear which data could be leaked in case of a cyber incident.	Obtain ethical approval and signed consent from parents and ensure that they know exactly what is involved in the evaluation.
Data minimisation	Do not collect any information that is not strictly required to authenticate the child.	Only collect data that is essential in terms of testing the usability of the authentication mechanism.
Data sharing	A child’s data can only be shared with explicit consent from the parents.	Provide data sharing information if the children are old enough to understand this.
Nudge techniques	Nudges must be used only be used for the good of the child, not for the good of the platform.	The mechanisms behind the nudge, as well as the anticipated influence of the nudge, must be explained to parents, and permission obtained to deploy the nudge with their children.
Online tools	Ensure that the child’s GDPR [European Union, 2018] rights are upheld, and that parents can satisfy themselves of this by including a link to terms and conditions and a contact email address in the interface.	Ensure that parents and children know how to access their children’s data and to exercise their GDPR rights in this respect. Ensure that the child is aware of their rights to their personal data before participation in evaluation.

Table 2: Technical Guidelines for designing & evaluating age-appropriate authentication mechanisms (The leftmost column emerged from our studies; In this Section,  $G_i$  refers to guidelines listed in Section 2.3,  $Q_i$  refers to image qualities derived in Section 7.1, and  $C_i$  refers to challenges mentioned in Section 7.2.)

Principle	Design	Evaluation
Use a tablet ( $G1$ , $G4$ )	This ensures that children unfamiliar with a mouse can devote all the cognitive bandwidth to using the mechanism	
Use age-appropriate image targets and distractors ( $G3$ , $G7$ , $G8$ , $Q1$ -5)	For the youngest children, maximise memorability and ease of use by using familiar images. For older children, generic images can indeed be used, but only when chosen with care. Ensure that the images you choose can be labelled uniquely by the target user group i.e. that the vocabulary and categorisation can be carried out by an average child of that age.	Memorability of images ought to be confirmed in a pilot study with the target demographic
Age-appropriate literacy requirements ( $G2$ )	Children in the 4-5 age group should not be required to identify themselves by entering a textual identifier such as an email address. Allowing children to choose ‘their’ image will work better. Older children may well be able to enter emails with ease.	Consult educators who will know average capabilities of children of each age group
Recruitment ( $C1$ )	Work with educational authorities to recruit children, or run cyber awareness events and evaluate new mechanisms as part of the event activities (within the ethical constraints laid out in Table 1).	
Hear the children’s voices ( $G6$ )	It is important to hear the children’s voices, respecting their opinions and perceptions of the authentication mechanisms we design for them. The second study used a questionnaire with questions and emoticons, which the researcher read out to the children, to gain their responses.	Pilot the questions with parents of children in your demographic to ensure that they are appropriate.
There are no short cuts ( $C2$ )	Evaluations of these mechanisms with children are going to take much longer than evaluations with adults. Expect that and do not try to speed things up. We did measure how long it took to authenticate, but we also pointed out that this was not realistic given the design of Kidzpass. The design specifically chose to randomise the appearance of target images rather than expect the child to identify the images in the correct sequence, which even adults find difficult to do	Prepare to spend as long as it takes and do not show impatience
Use free software ( $C3$ )	KidzPass was developed using Django, a free python-based web development framework. All images used as identifiers were free. All the images used in the final study were free images, not requiring copyrighting. This ensures that any adopter can use it because financial limitations do not deter usage	Ensure that all images are free to use, and that software subscriptions are not required.

*Facilitating existing authentication replacement:* Passwords are integrated into the software used within schools. While educational authorities might be well disposed towards their replacement for young users, the change process needs to be as easy as possible. It might be necessary to provide a plug-and-play authentication mechanism to make the replacement of the password as viable as possible.

*Supporting teachers:* Teachers are not cyber security experts and cope the best way they can. As a community, we need to provide more resources to teachers both to ensure that they understand password ‘best practice’ and to help them to convey these principles to the children in their care. Initial steps in this direction have already been made, and can be accessed from <https://cybersquad.uk>.

*Accessible authentication for young children:* KidzPass can clearly only be used by sighted children. There is a need for alternatives to passwords that can be accessible to children with vision difficulties as well.

## Acknowledgements

We acknowledge the contributions of Michaela Stewart and Mhairi Campbell, the researchers who carried out the two KidzPass studies, and Suzy Prior, who was an essential contributor to the design and evaluation processes. We also thank all the wonderful children who took part in our studies. This research was supported by the Helmholtz Association (HGF) through the subtopic Engineering Secure Systems (ESS). Parts of the project were funded by the International Excellence Grants and Fellowships Programme of Karlsruhe Institute of Technology (KIT). Karen Renaud was successfully nominated as KIT International Excellence Fellow for 2021.

## References

- [Alkhamis et al., 2020] Alkhamis, E., Petrie, H., and Renaud, K. (2020). Kidsdoodlepass: an exploratory study of an authentication mechanism for young children. In *HAISA, Mytilene, Greece, 7-9 July 2021*, pages 123–132. Springer International Publishing.
- [Anagnostaki et al., 2013] Anagnostaki, L., Wright, M. J., and Papathanasiou, A. (2013). Secrets and disclosures: How young children handle secrets. *The Journal of Genetic Psychology*, 174(3):316–334.
- [Assal et al., 2018] Assal, H., Imran, A., and Chiasson, S. (2018). An exploration of graphical password authentication for children. *International Journal of Child-Computer Interaction*, 18:37–46.

- [Barrett, 2017] Barrett, L. F. (2017). *How emotions are made: The secret life of the brain*. Houghton Mifflin, Harcourt, New York.
- [Biddle et al., 2012] Biddle, R., Chiasson, S., and van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys*, 44(4):1–41.
- [Bjorklund and Zaken-Greenberg, 1981] Bjorklund, D. F. and Zaken-Greenberg, F. (1981). The effects of differences in classification style on preschool children’s memory. *Child Development*, pages 888–894.
- [Bosse and Valdois, 2009] Bosse, M.-L. and Valdois, S. (2009). Influence of the visual attention span on child reading performance: a cross-sectional study. *Journal of Research in Reading*, 32(2):230–253.
- [Brostoff and Sasse, 2000] Brostoff, S. and Sasse, M. A. (2000). Are Passfaces more usable than passwords? A field trial investigation. In *People and computers XIV — Usability or Else!*, pages 405–424. Springer.
- [Brown and Campione, 1972] Brown, A. L. and Campione, J. C. (1972). Recognition memory for perceptually similar pictures in preschool children. *Journal of Experimental Psychology*, 95(1):55–62.
- [Brown and Scott, 1971] Brown, A. L. and Scott, M. S. (1971). Recognition memory for pictures in preschool children. *Journal of Experimental Child Psychology*, 11(3):401–412.
- [Cain and Still, 2018] Cain, A. A. and Still, J. D. (2018). Usability comparison of over-the-shoulder attack resistant authentication schemes. *Journal of Usability Studies*, 13(4):196–219.
- [Chiasson et al., 2007] Chiasson, S., van Oorschot, P. C., and Biddle, R. (2007). Graphical password authentication using cued click points. In *European Symposium on Research in Computer Security*, pages 359–374.
- [ChildTrends, 2018] ChildTrends (2018). Home Computer Access and Internet Use. <https://www.childtrends.org/indicators/home-computer> Accessed: April 07, 2019.
- [Choong et al., 2019] Choong, Y.-Y., Theofanos, M., Renaud, K., and Prior, S. (2019). Case Study – Exploring Children’s Password Knowledge and Practices. In *Usable Security (USEC)*. San Diego, February.
- [Chowdhury et al., 2013] Chowdhury, S., Poet, R., and Mackenzie, L. (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*, pages 768–775. IEEE.

- [Chu et al., 2020] Chu, X., Sun, H., and Chen, Z. (2020). Passpage: Graphical password authentication scheme based on web browsing records. In *International Conference on Financial Cryptography and Data Security*, pages 166–176. Springer.
- [Coggins III, 2013] Coggins III, P. E. (2013). Implications of what children know about computer passwords. *Computers in the Schools*, 30(3):282–293.
- [Cordon et al., 2013] Cordon, I. M., Melinder, A. M., Goodman, G. S., and Edelstein, R. S. (2013). Children’s and adults’ memory for emotional pictures: Examining age-related patterns using the Developmental Affective Photo System. *Journal of Experimental Child Psychology*, 114(2):339–356.
- [Corsini et al., 1969] Corsini, D. A., Jacobus, K. A., and Leonard, S. D. (1969). Recognition memory of preschool children for pictures and words. *Psychonomic Science*, 16(4):192–193.
- [Cowan et al., 2011] Cowan, N., AuBuchon, A. M., Gilchrist, A. L., Ricker, T. J., and Saults, J. S. (2011). Age differences in visual working memory capacity: Not based on encoding limitations. *Developmental Science*, 14(5):1066–1074.
- [Curtin, 2001] Curtin, C. (2001). Eliciting children’s voices in qualitative research. *American Journal of Occupational Therapy*, 55(3):295–302.
- [Cycowicz et al., 2001] Cycowicz, Y. M., Friedman, D., Snodgrass, J. G., and Duff, M. (2001). Recognition and source memory for pictures in children and adults. *Neuropsychologia*, 39(3):255–267.
- [Darbanian et al., 2015] Darbanian, E. et al. (2015). A graphical password against spyware and shoulder-surfing attacks. In *2015 International Symposium on Computer Science and Software Engineering (CSSE)*, pages 1–6. IEEE.
- [de Haan et al., 2001] de Haan, M., Johnson, M. H., Maurer, D., and Perrett, D. I. (2001). Recognition of individual faces and average face prototypes by 1-and 3-month-old infants. *Cognitive Development*, 16(2):659–678.
- [Dhamija and Perrig, 2000] Dhamija, R. and Perrig, A. (2000). Deja vu: A user study using images for authentication. In *USENIX Security Symposium*, pages 45–58.
- [Duncan et al., 1994] Duncan, J., Ward, R., and Shapiro, K. (1994). Direct measurement of attentional dwell time in human vision. *Nature*, 369(6478):313–315.
- [Dunphy et al., 2008] Dunphy, P., Nicholson, J., and Olivier, P. (2008). Securing passfaces for description. In *Proceedings of the 4th symposium on Usable Privacy and Security*, pages 24–35.

- [Ebbinghaus, 1885] Ebbinghaus, H. (1885). *Über das gedächtnis: untersuchungen zur experimentellen psychologie*. Duncker & Humblot.
- [Ehri, 1995] Ehri, L. C. (1995). Phases of development in learning to read words by sight. *Journal of Research in Reading*, 18(2):116–125.
- [European Union, 2018] European Union (2018). General data protection regulation gdpr. Retrieved 20 Feb 2021 from: <https://gdpr-info.eu/>.
- [Fernandes et al., 2018] Fernandes, M. A., Wammes, J. D., and Meade, M. E. (2018). The surprisingly powerful influence of drawing on memory. *Current Directions in Psychological Science*, 27(5):302–308.
- [Filan and Sullivan, 1980] Filan, G. and Sullivan, H. (1980). Effects of induced memory strategies on children’s memory for pictures and words. In *Annual Educational Research Association Annual Convention*, Boston, USA.
- [Fioravanti et al., 1995] Fioravanti, F., Inchingolo, P., Pensiero, S., and Spanio, M. (1995). Saccadic eye movement conjugation in children. *Vision Research*, 35(23-24):3217–3228.
- [Frey and Bosse, 2018] Frey, A. and Bosse, M.-L. (2018). Perceptual span, visual span, and visual attention span: Three potential ways to quantify limits on visual processing during reading. *Visual Cognition*, 26(6):412–429.
- [Gathercole, 1999] Gathercole, S. E. (1999). Cognitive approaches to the development of short-term memory. *Trends in Cognitive Sciences*, 3(11):410–419.
- [Gobbini and Haxby, 2007] Gobbini, M. I. and Haxby, J. V. (2007). Neural systems for recognition of familiar faces. *Neuropsychologia*, 45(1):32–41.
- [Henson et al., 2000] Henson, R., Shallice, T., and Dolan, R. (2000). Neuroimaging evidence for dissociable forms of repetition priming. *Science*, 287(5456):1269–1272.
- [Herley and van Oorschot, 2012] Herley, C. and van Oorschot, P. (2012). A Research Agenda Acknowledging the Persistence of Passwords. *IEEE Security & Privacy*, 10(1):28–36.
- [Hitch and Halliday, 1983] Hitch, G. and Halliday, M. (1983). Working memory in children. *Philosophical Transactions of the Royal Society of London. B, Biological Sciences*, 302(1110):325–340.
- [Hitch et al., 1988] Hitch, G. J., Halliday, S., Schaafstal, A. M., and Schraagen, J. M. C. (1988). Visual working memory in young children. *Memory & Cognition*, 16(2):120–132.



- [Hlywa et al., 2011] Hlywa, M., Biddle, R., and Patrick, A. S. (2011). Facing the facts about image type in recognition-based graphical passwords. In *Annual Computer Security Applications Conference*, pages 149–158.
- [Information Commissioner’s Office, 2020] Information Commissioner’s Office (2020). Age appropriate design: a code of practice for online services. Retrieved 8 February from:  
<https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/>.
- [ISO, 2018] ISO (2018). Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts. <https://www.iso.org/standard/63500.html>.
- [Jenkins et al., 2014] Jenkins, R., McLachlan, J. L., and Renaud, K. (2014). Facelock: familiarity-based graphical authentication. *PeerJ*, 2:e444.
- [Jermyn et al., 1999] Jermyn, I., Mayer, A., Monroe, F., Reiter, M. K., and Rubin, A. D. (1999). The design and analysis of graphical passwords. In *USENIX Association*.
- [Karras et al., 2020] Karras, T., Laine, S., Aittala, M., Hellsten, J., Lehtinen, J., and Aila, T. (2020). Analyzing and Improving the Image Quality of StyleGAN. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 8110–8119.  
<https://arxiv.org/pdf/1912.04958.pdf>.
- [King, 1991] King, M. M. (1991). Rebus passwords. In *Annual Computer Security Applications Conference*, pages 239–243, San Antonio, TX, USA.
- [Knoblich and Prinz, 2001] Knoblich, G. and Prinz, W. (2001). Recognition of self-generated actions from kinematic displays of drawing. *Journal of Experimental Psychology: Human Perception and Performance*, 27(2):456.
- [Li et al., 2005] Li, Z., Sun, Q., Lian, Y., and Giusto, D. D. (2005). An association-based graphical password design resistant to shoulder-surfing attack. In *2005 IEEE international conference on multimedia and expo*, pages 245–248. IEEE.
- [Marques, 2007] Marques, J. F. (2007). Unlearning: The Hardest Lesson of All. *Performance Improvement*, 46(1):5–6.
- [Mayer, 2019] Mayer, P. (2019). *Secure and Usable User Authentication*. PhD thesis, Karlsruhe Institute of Technology.

- [Mayer et al., 2014] Mayer, P., Volkamer, M., and Kauer, M. (2014). Authentication Schemes - Comparison and Effective Password Spaces. In *International Conference on Information System Security*, pages 204–225, Hyderabad, India.
- [Mendori et al., 2002] Mendori, T., Kubouchi, M., Okada, M., and Shimizu, A. (2002). Password input interface suitable for primary school children. In *International Conference on Computers in Education*, pages 765–766, Auckland, New Zealand. IEEE.
- [Mihajlov and Jerman-Blazic, 2018] Mihajlov, M. and Jerman-Blazic, B. (2018). Eye tracking graphical passwords. In Magnaghi-Delfino, P. and Norando, T., editors, *Advances in Intelligent Systems and Computing*, page 37–44, San Diego, CA, USA. Springer.
- [Moore et al., 2008] Moore, T., McArthur, M., and Noble-Carr, D. (2008). Little voices and big ideas: Lessons learned from children about research. *International Journal of Qualitative Methods*, 7(2):77–91.
- [Mulhall, 1915] Mulhall, E. F. (1915). Experimental Studies in Recall and Recognition. *The American Journal of Psychology*, 26(2):217–228.
- [Munoz et al., 1998] Munoz, D., Broughton, J., Goldring, J., and Armstrong, I. (1998). Age-related performance of human subjects on saccadic eye movement tasks. *Experimental Brain Research*, 121(4):391–400.
- [Murphy-Berman et al., 1986] Murphy-Berman, V., Rosill, J., and Wright, G. (1986). Measuring children’s attention span: A microcomputer assessment technique. *The Journal of Educational Research*, 80(1):23–28.
- [Nelson et al., 1976] Nelson, D. L., Reed, V. S., and John R, W. (1976). Pictorial Superiority Effect. *Journal of Experimental Psychology: Human Learning and Memory*, 2:523–528.
- [Ornstein and Naus, 1985] Ornstein, P. A. and Naus, M. J. (1985). Effects of the knowledge base on children’s memory strategies. *Advances in Child Development and Behavior*, 19:113–148.
- [Paivio and Csapo, 1973] Paivio, A. and Csapo, K. (1973). Picture superiority in free recall: Imagery or dual coding? *Cognitive Psychology*, 5(2):176–206.
- [Paivio et al., 1968] Paivio, A., Rogers, T. B., and Smythe, P. C. (1968). Why are pictures easier to recall than words? *Psychonomic Science*, 11:137–138.
- [Peskin and Ardino, 2003] Peskin, J. and Ardino, V. (2003). Representing the mental world in children’s social behavior: Playing hide-and-seek and keeping a secret. *Social Development*, 12(4):496–512.

- [Prior and Renaud, 2020] Prior, S. and Renaud, K. (2020). Age-appropriate password “best practice” ontologies for early educators and parents. *International Journal of Child-Computer Interaction*, 23–24. <https://doi.org/10.1016/j.ijcci.2020.100169>.
- [Ratakonda et al., 2019] Ratakonda, D. K., French, T., and Fails, J. A. (2019). “My Name is My Password:” Understanding Children’s Authentication Practices. In *Proceedings of the 18th ACM International Conference on Interaction Design and Children*, pages 501–507, June 12–15, Boise, ID, USA.
- [Read and Cassidy, 2012] Read, J. C. and Cassidy, B. (2012). Designing textual password systems for children. In *Proceedings of the 11th International Conference on Interaction Design and Children*, pages 200–203, Bremen, Germany. ACM.
- [Reese, 1975] Reese, H. W. (1975). Verbal effects in children’s visual recognition memory. *Child Development*, 46(2):400–407.
- [Renaud, 2009a] Renaud, K. (2009a). Guidelines for designing graphical authentication mechanism interfaces. *International Journal of Information and Computer Security*, 3(1):60–85.
- [Renaud, 2009b] Renaud, K. (2009b). Web authentication using Mikon images. In *2009 World Congress on Privacy, Security, Trust and the Management of e-Business*, pages 79–88, St Johns, Canada. IEEE.
- [Renaud and Maguire, 2009] Renaud, K. and Maguire, J. (2009). Armchair authentication. *People and Computers XXIII Celebrating People and Technology*, pages 388–397.
- [Renaud et al., 2013] Renaud, K., Mayer, P., Volkamer, M., and Maguire, J. (2013). Are graphical authentication mechanisms as strong as passwords? In *2013 Federated Conference on Computer Science and Information Systems*, pages 837–844. IEEE.
- [Shammee et al., 2020] Shammee, T. I., Akter, T., Mou, M., Chowdhury, F., and Ferdous, M. S. (2020). A Systematic Literature Review of Graphical Password Schemes. *J. Comput. Sci. Eng.*, 14:163–185.
- [Siegler, 2013] Siegler, R. (2013). *Children’s thinking: what develops?* Psychology Press, Hillsdale, New Jersey.
- [Sowell et al., 2004] Sowell, E. R., Thompson, P. M., Leonard, C. M., Welcome, S. E., Kan, E., and Toga, A. W. (2004). Longitudinal mapping of cortical thickness and brain growth in normal children. *Journal of Neuroscience*, 24(38):8223–8231.

- [Stewart et al., 2020] Stewart, M., Campbell, M., Renaud, K., and Prior, S. (2020). Kidzpass: authenticating pre-literate children. In *2020 Dewald Roode Workshop on Information Systems Security Research*. IFIP Working Group 8.11/11.13.
- [Suo et al., 2005] Suo, X., Zhu, Y., and Owen, G. S. (2005). Graphical Passwords: A Survey. In *Annual Computer Security Applications Conference*, pages 472–481, Tucson, AZ, USA.
- [Tversky, 1973] Tversky, B. (1973). Encoding Processes in Recognition and Recall. *Cognitive Psychology*, 5(3):275–287.
- [Weinshall, 2006] Weinshall, D. (2006). Cognitive authentication schemes safe against spyware. In *Symposium on Security and Privacy (S&P’06)*, pages 295–300. IEEE.
- [Weithorn, 1983] Weithorn, L. A. (1983). Involving children in decisions affecting their own welfare. In *Children’s Competence to Consent*, pages 235–260. Springer.
- [Williams, 2015] Williams, A. D. (2015). The development of a music program to improve the attention span of school-aged children. Master’s thesis, Capella University.
- [Yan et al., 2004] Yan, J., Blackwell, A., Anderson, R., and Grant, A. (2004). Password memorability and security: empirical results. *IEEE Security & Privacy*, 2(5):25–31.
- [Yang, 2017] Yang, G. (2017). Passpositions: A secure and user-friendly graphical password scheme. In *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*, pages 1–5.
- [Zhang-Kennedy et al., 2016] Zhang-Kennedy, L., Mekhail, C., Abdelaziz, Y., and Chiasson, S. (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*, pages 388–399.
- [Zimmermann and Gerber, 2020] Zimmermann, V. and Gerber, N. (2020). The password is dead, long live the password—a laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies*, 133:26–44.
- [Zwiers and Morrisette, 2013] Zwiers, M. and Morrisette, P. J. (2013). *Effective interviewing of children: A comprehensive guide for counselors and human service workers*. Taylor & Francis, Philadelphia, USA.