AIS Transactions on Human-Computer Interaction

Volume 13 | Issue 4 Article 2

12-31-2021

Principles for Designing Authentication Mechanisms for Young Children: Lessons Learned from KidzPass

Karen Renaud
University of Strathclyde, karen.renaud@strath.ac.uk

Melanie Volkamer
Karlsruhe Institute of Technology (KIT), melanie.volkamer@kit.edu

Peter Mayer
Karlsruhe Institute of Technology, peter.mayer@kit.edu

Rüdiger Grimm
Fraunhofer Institute for Secure IT and Christian-Morgenstern-Schule Darmstadt, ruediger.grimm@sit.fraunhofer.de

Recommended Citation

Renaud, K., Volkamer, M., Mayer, P., & Grimm, R. (2021). Principles for Designing Authentication Mechanisms for Young Children: Lessons Learned from KidzPass. *AIS Transactions on Human-Computer Interaction, 13*(4), 407-430. https://doi.org/10.17705/1thci.00155
DOI: 10.17705/1thci.00155

Transactions on Human-Computer Interaction

Volume 13 Issue 4

12-2021

Principles for Designing Authentication Mechanisms for Young Children: Lessons Learned from KidzPass

Karen Renaud

Department of Computer and Information Sciences, University of Strathclyde, karen.renaud@strath.ac.uk

Department of Information Systems, Rhodes University, South Africa

School of Computing, University of South Africa, South Africa

Melanie Volkamer

Security - Usability - Society, Karlsruhe Institute of Technology, melanie.volkamer@kit.edu

Peter Mayer

Security - Usability - Society, Karlsruhe Institute of Technology, peter.mayer@kit.edu

Rüdiger Grimm

Fraunhofer Institute for Secure IT and Christian-Morgenstern-Schule Darmstadt, ruediger.grimm@sit.fraunhofer.de

Recommended Citation

Renaud, K., Volkamer, M., Mayer, P., & Grimm, R. (2021). Principles for designing authentication mechanisms for young children: Lessons learned from KidzPass. *AIS Transactions on Human-Computer Interaction*, *13*(4), pp. 407-430.

DOI: 10.17705/1thci.00155

Available at http://aisel.aisnet.org/thci/vol13/iss4/2

Transactions on Human-Computer Interaction

Research Paper DOI: 10.17705/1thci.00155 ISSN: 1944-3900

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

Karen Renaud
Department of Computer and Information Sciences,
University of Strathclyde

Melanie Volkamer
Security - Usability - Society,
Karlsruhe Institute of Technology

Peter Mayer
Security - Usability - Society,
Karlsruhe Institute of Technology

Rüdiger Grimm
Fraunhofer Institute for Secure IT and Christian-Morgenstern-Schule Darmstadt

Abstract:

Young children routinely authenticate themselves with alphanumeric passwords but are probably not ready to use such passwords due to their emerging literacy and immaturity. They might adopt insecure coping tactics, which could become entrenched. Because children have a superior pictorial recognition ability, graphical authentication mechanisms will likely represent more suitable mechanisms for this demographic. We propose and study KidzPass, a configurable graphical authentication framework that one can use to tailor these mechanisms for children of different ages. We carried out two empirical investigations with four- to five-year-old children and with six- to seven-year-old children using personalized images as secrets (familiar faces and self-drawn doodles). KidzPass proved efficacious and our younger (four- to seven-year-old) participants mostly preferred it to text passwords. The personalized images maximize memorability but take significant time to obtain. As children mature, it might be possible to replace personalized images with generic images. Thus, we carried out a final empirical study with older children using generic images (that we chose). From this study, we found that 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 efforts to design and evaluate age-appropriate authentication mechanisms for young children both from an ethical and technical perspective.

Keywords: Children, Authentication, Design Principles, Ethics.

Mala Kaul was the accepting senior guest editor for this paper.

1 Introduction

Computer users traditionally authenticate their identity in three different ways based on: 1) what they know, 2) what they hold, and 3) what they are. Most users prefer the first form: a shared secret, essentially a string of alphanumeric and/or special characters (Zimmermann & Gerber, 2020). A shared secret confirms the user's claimed identity in order to permit access to information, resources, or services. As technology has diffused into schools and the coronavirus disease of 2019 (COVID-19) pandemic has forced children to use the Internet during homeschooling, children now use passwords from a very young age (ChildTrends, 2018). Users should: 1) memorize, 2) not divulge, and 3) be able to enter passwords correctly. A young child might struggle to meet these requirements even more so than adults do.

With respect to memorizing passwords, 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 recognize and name letters. Children do not reach adult levels of retention ability until adolescence (Sowell et al., 2004). With respect to keeping passwords secret, young children cannot necessarily distinguish between people they can share their secrets with and people they should not (Anagnostaki, Wright, & Papathanasiou, 2013). This conflict might confuse them. With respect to entering passwords, the password owner has to be able to parse words into individual characters. To do so, they have to mentally track the character position in the password and advance the position as they type each letter. Young children have likely not adequately formed this ability due to their shorter attention spans (Frey & Bosse, 2018). Moreover, consider that the keyboards display letters in upper case; however, when one presses it, it produces a lower case letter and likely a letter in a serif font, which differs from what children typically learn to write. Children also receive no visual feedback to help them to confirm that they have entered the password correctly.

Because children use passwords before they have the requisite skills, they do not necessarily know how to cope (Choong, Theofanos, Renaud, & Prior, 2019) and likely struggle to create, retain, and manage passwords (Prior & Renaud, 2020). They might engage in insecure behaviors, such as reusing passwords or writing them down (Ratakonda, French, & Fails, 2019). Since people find it hard to unlearn a bad habit once it has become established (Marques, 2007), we believe that identifying an age-appropriate alternative mechanism that better suits children would prove valuable.

Alternatives should rely on knowledge about 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, Rogers, & Smythe, 1968). We have reason to believe that they could be suitable for young children to use (Renaud, 2009b; Alkhamis, Petrie, & Renaud, 2020) since evidence has shown that children can remember pictures better than text (Corsini, Jacobus, & Leonard, 1969; Brown & Campione, 1972; Filan & Sullivan, 1980).

With this study, we make several contributions. First, we propose a framework for informing the choice of graphical authentication mechanism configuration for children of different ages. Second, we detail three studies we carried out with KizPass instantiations. Third, we provide a set of ethical design principles for age-appropriate graphical authentication schemes grounded in the United Kingdom's "Age Appropriate Design Standard" published in September 2020 (Information Commissioner's Office, 2020) (see Table 1) and technical design principles for age-appropriate graphical authentication design that we derived from 1) guidelines we obtained from the research literature, 2) challenges that emerged from the KidzPass evaluations, and 3) qualities that contribute towards generic images' memorability.

This paper proceeds as follows: In Section 2, we review the latest research in the graphical authentication area. In Section 3, we enumerate the insights that we gained from such research to create an alternate authentication mechanism for young children that we call the KidzPass framework, demonstrate how one can configure it depending on the target user group's age, and introduce three research questions. In Sections 4 to 6, we report on empirical investigations that we conducted to address the research questions. In Section 7, we reflect on our investigations to answer our research questions and discuss lessons learned. In Section 8, we synthesize our findings to create principles to inform future research in this space. Finally, in Section 9, we conclude the paper. We graphically depict the paper's structure in Figure 1.

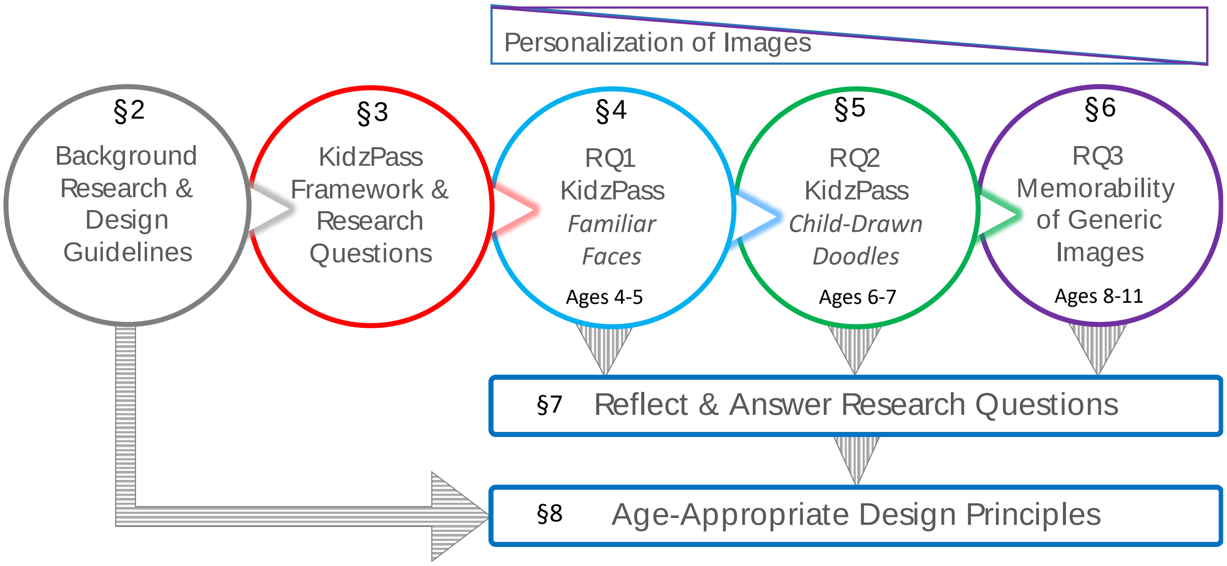

Personalization of Images
§2
Background Research & Design Guidelines
§3
KidzPass Framework & Research Questions
§4
RQ1
KidzPass
Familiar Faces
Ages 4-5
§5
RQ2
KidzPass
Child-Drawn Doodles
Ages 6-7
§6
RQ3
Memorability of Generic Images
Ages 8-11
§7 Reflect & Answer Research Questions
§8 Age-Appropriate Design Principles

Figure 1. Paper Structure

2 Graphical Authentication Research

People originally conceived alphanumeric passwords to authenticate technophiles in the mainframe computer era. Today, they constitute the dominant authentication mechanism across the world (Herley & van Oorschot, 2012). Due to this mismatch between alphanumeric passwords' original target audience and their actual users today, people deploy coping skills to offset the human memorial burden that they impose, which weakens the mechanism. The graphical authentication mechanism represents one alternative to alphanumeric passwords (Biddle, Chiasson, & van Oorschot, 2012). These mechanisms rely on the so-called pictorial superiority effect (Nelson, Reed, & John, 1976). Paivio's dual-coding theory (Paivio et al., 1968) posits that the human brain processes and stores visual information differently from random alphanumeric strings, which means that people are more likely to remember pictures. In this way, graphical authentication mechanisms should enhance the extent to which people can remember authentication secrets.

2.1 Basics

The research literature has proposed myriad graphical authentication mechanisms (Suo, Zhu, & Owen, 2005; Mayer, Volkamer, & Kauer, 2014; Biddle et al., 2012), which we can categorize into three categories based on the memory technique they require (Biddle et al., 2012): 1) uncued recall-based mechanisms, 2) cued recall-based mechanisms, and 3) recognition-based mechanisms.

When using uncued recall-based mechanisms, users recall the entire secret and enter it in a predefined blank field (e.g., an empty field for a text-based password and a blank canvas for graphical authentication mechanisms). Mechanisms in this category place the most cognitive demand on users, and users experience the greatest memorability issues when dealing with them (Yan, Blackwell, Anderson, & Grant, 2004, Mulhall, 1915). Example mechanisms in this category include Jermyn, Mayer, Monrose, Reiter, and Rubin's (1999) traditional draw-a-secret mechanism and other more recent proposals (Yang, 2017).

Cued recall-based mechanisms improve memorability by providing cues to help users recall the authentication secret. Example mechanisms in this category include rebus passwords (King, 1991), the cued click points mechanism (Chiasson, Van Oorschot, & Biddle, 2007), and Weinshall's (2006) cognitive mechanism.

Recognition-based authentication mechanisms generally display one or more "challenge sets" that each contains one target image and several distractor images. Users have to identify "their" target image from each challenge set. Mechanisms in this category place much less cognitive demand on users than uncued recall- or cued recall-based mechanisms (Mulhall, 1915; Tversky, 1973) and, thus, attract fewer authentication failures than passwords (Mayer et al., 2014, Dhamija & Perrig, 2000; Brostoff & Sasse, 2000) and memorability advantages (e.g., Hlywa, Biddle, & Patrick, 2011; Dhamija & Perrig, 2000). The system can randomly assign the “secret” target images (Brostoff & Sasse, 2000), the user can choose them (Renaud & Maguire, 2009), the user can provide them (Jenkins, McLachlan, & Renaud, 2014), or the system can draw them from websites in the user’s browsing history (Chu, Sun, & Chen, 2020). Distractor images have to be chosen with care so that they do not resemble the target image too closely so as not to interfere with target identification.

2.2 Child-Specific Graphical Authentication

We have argued for using an alternative to alphanumeric passwords until children have developed sufficiently to be able to manage text passwords. Researchers have widely studied graphical authentication mechanisms (e.g., Biddle et al., 2012; Shammee, Akter, Mou, Chowdhury, & Ferdous, 2020) and their design dimensions (e.g., Renaud, 2009a) but not for this age group. Before exploring the literature that addresses children’s graphical authentication mechanisms, we first address the viability of the other two kinds of authentication from a child’s perspective: 1) “something you are” (i.e., biometrics) and 2) “something you hold”. The first does not suit children because it can violate their privacy, and biometric readers are not as ubiquitous as keyboards and trackpads/mice. The “something you hold” option would require children to look after a dongle or other device that they can demonstrate they own to authenticate themselves. However, they may not be mature enough to take do so or to prevent older children from appropriating them.

We now review graphical authentication mechanisms that researchers have evaluated with children. Read and Cassidy (2012) and Coggins (2013) investigated 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 six- to 10-year-old children and Coggins surveyed nine- to 12-year-old children. While these studies have identified valuable insights, due to the speed at which children develop, we do not know whether these findings remain valid for four- to five-year-old children who mostly lack literacy skills.

Assal, Imran, and Chiasson (2018) did extensive research into using the PassTiles graphical password mechanism as an alternative authentication method for children. In their study, they investigated three variants of the mechanism and provided recommendations for designing more child-friendly authentication methods. They explored their results through user performance and, overall, largely successfully suggested that both groups in the study (i.e., 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, Kubouchi, Okada, and Shimizu (2002) examined password use in Japanese primary schools. They highlighted that, at the time they conducted their study, users needed to enter their names and passwords using alphanumeric characters on a keyboard to authenticate themselves. Japanese primary school children find this system rather difficult given they have yet to learn the Roman alphabet. Therefore, the authors conducted a project to design a new interface using symbols the children were more familiar with. They then altered the system by changing factors such as the number of icons and icon-selection time. They designed a mouse-based system with the icons appearing on the screen arranged randomly to avoid the possibility that one could distinguish passwords from the position at which icons appeared on the screen. Users inputted passwords using buttons. They tested three types of interfaces with different numbers of icons. They did not state how many subjects they tested each interface with or their age. However, they evaluated the system based on the number of correct selections and the average input time. They found that children performed best when the system displayed 16 icons and three challenge sets. Based on these results, we cannot easily assess whether the children found the second interface the best without hearing their opinions about the mechanism.

The obvious criticisms of graphical authentication mechanisms include the fact that they lack dictionaries 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 poses a risk (Darbanian & Fard, 2015; Li, Sun, Lian, & Giusto, 2005). These mechanisms admittedly lack the strength that text passwords offer (Renaud, Mayer, Volkamer, & Maguire, 2013). However, if we consider the context in which children use passwords, these issues become less significant. In the first place, four- to five-year-old children can likely manage only weak textual passwords, and a graphical password can easily provide better security. Moreover, research has shown that adults and children tend to prefer graphical authentication mechanisms (Assal et al., 2018), which seem particularly suitable for use in low-risk systems where mechanisms protect information that has little value. One can, however, usefully deploy such graphical authentication mechanisms to teach children authentication principles.

2.3 Design and Evaluation Guidelines

An age-appropriate graphical authentication mechanism could represent an alternative to password authentication for young children. Such a mechanism would likely more effectively accommodate different levels of literacy and emerging maturity than textual passwords. In Sections 2.3.1 to 2.3.8, we provide some pertinent design guidelines that such a mechanism should follow (extended from Stewart, Campbell, Renaud, & Prior, 2020). We number the guidelines in parentheses to be able to refer back to them later in the paper.

2.3.1 Technological Naivety (G1)

Fortunate children have computers in their homes, but not all will have this advantage. Some may never have used a keyboard, so we cannot assume that the children will be able to use one proficiently. Moreover, if a child is accustomed to a tablet, using a computer 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.

2.3.2 Emerging Literacy (G2)

Children proceed through several 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 et al. (2002) suggested using images instead of passwords. Hence, in designing the alternative authentication mechanism user interface, the use of text should be minimized.

2.3.3 Ability to Retain Information Long Term (G3)

Users have to retain passwords for variable periods of time. Given the admonition not to write passwords down, users require long-term memory skills to remember them (Gathercole, 1999; Sowell et al., 2004). Hence, we ought to use images that maximize memorability: something personal to children or something they provide.

2.3.4 Ability to Interact without Feedback (G4)

Entering a password requires a person to enter the characters one at a time while maintaining the position in their password in their minds. They have to perform this process without any visual feedback. While adults can do it, young children do not necessarily have these skills yet (Cowan, AuBuchon, Gilchrist, Ricker, & Saults, 2011). In this regard, being able to recognize images rather than entering a password represents a better option (Mendori et al., 2002; Assal et al., 2018). Hence, once again, the mechanism should not rely on children to rely on their still immature sequential memory. Hence, we should not require them to remember images in sequence but only the images themselves.

2.3.5 Secret Keeping (G5)

A cardinal rule states that people should keep their passwords a secret. Yet, young children cannot necessarily keep secrets from their friends (Peskin & Ardino, 2003; Anagnostaki et al., 2013). Moreover, for children, this admonition involves more nuance than it does for adults because children ought to share their passwords with their teachers and caregivers but not with other children or other adults. The ability to make these distinctions requires a maturity that young children have likely not yet attained. In their study with children, Zhang-Kennedy, Mekhail, Abdelaziz, and Chiasson (2016) discovered that the children did not understand the need to keep their passwords secret, which confirms this difficulty. Thus, once again, we see the need to use something that children cannot easily describe to others—one cannot describe a face or drawing as easily as telling someone a textual password (Dunphy, Nicholson, & Olivier, 2008; Chowdhury, Poet, & Mackenzie, 2013).

2.3.6 Listen to Children (G6)

Curtin (2001) and Moore, McArthur, and Noble-Carr (2008) have highlighted the need to hear children's voices when involving them in research. Curtin (2001, p. 299) noted:

> *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*.

Curtin offered various recommendations for designing activities to help children to express their opinions, such as 1) giving them time to settle down in a quiet environment, 2) asking questions while they participate 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 insufficient understanding so that they can bring the evaluation to a close.

2.3.7 Limited Attention Span (G7)

Children (especially younger children and children who suffer from a range of neurological difficulties such as attention deficit syndrome (Williams, 2015)) have a poorly formed ability to focus, especially in terms of visual attention, but they develop the ability quickly as they learn to read (Bosse & Valdois, 2009; Murphy-Berman, Rosill, & Wright, 1986). Hence, one should not expect children in the youngest age group should to have a greater visual attention span than their age suggests.

2.3.8 Visual Acuity (G8)

Studies have identified age-related changes in recognition dwell time (Fioravanti, Inchingolo, Pensiero, & Spanio, 1995; Duncan, Ward, & Shapiro, 1994; Murphy-Berman et al., 1986) and in saccadic task performance (Munoz, Broughton, Goldring, & Armstrong, 1998), which means that we cannot overload children's visual centers 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, graphical authentication challenge sets, especially for the youngest group, should not include too many images.

3 The KidzPass Framework

We propose a graphical authentication for children that relies on image recognition and exploits the picture superiority effect (Paivio & Csapo, 1973). Such authentication addresses G1, G3, and G4 above. Moreover, it limits the possibility for children to tell others their authentication secrets. However, we also know that children develop rapidly and learn new skills very fast (G2, G5, G7, & G8). Hence, we suggest a configurable framework that can ensure the deployed authentication mechanism matches a child's existing development stage. We now describe the different configuration aspects:

Interface: G2 requires that one use icons rather than text, especially for the four- to five-year-old age group and the six- to seven-year-old age group.

Identification: As children in the first two age groups have not yet become literate, we cannot expect them to enter an email address to identify themselves. Thus, we can configure the system to provide a clipart-type image of an animal that children can choose to identify with (one that other children have not selected). The oldest group, having learned how to read and write, can use a personal user name.

Authentication image type: (refer to G3)

- Four- to five-year-old age group: People can naturally remember faces and master face recognition at a very young age (de Haan, Johnson, Maurer, & Perrett, 2001; Barrett, 2017). Moreover, Cordon, Melinder, Goodman, and Edelstein (2013) found that children remember high and moderate arousal images more accurately than low arousal images and that familiar faces trigger more arousal than unfamiliar ones (Henson, Shallice, & Dolan, 2000). Thus, for four- to five-year-old children, KidzPass uses familiar faces to maximize memorability.
- Six- to seven-year-old age group: For this group, KidzPass uses children's own drawn doodles. Other studies have also used doodles with children, such as with pre-teens (Renaud, 2009b) and children slightly older than pre-teens (Alkhamis et al., 2020). Such images have superior

memorability due to the action planning memory they invoke when viewed again (Fernandes, Wammes, & Meade, 2018; Knoblich & Prinz, 2001).

- Eight- to nine-year-old age group: For this group, KidzPass uses generic images. Using generic images enhances scalability for an age group that has reached sufficient maturity as to not require personalized images. One should assign these images ought to children rather than permitting them to choose to reduce guessability (Cain & Still, 2018).

Challenge set size: (refer to G7, G8) The guidelines for adults provide warnings against a challenge set with too many images (Renaud, 2009a), which becomes an even bigger issue for child-specific challenge sets. On the other hand, a challenge set that contains only six images as Mihajlov and Jerman-Blazic (2018) have suggested would make it far too easy for another child to subvert the access-control mechanism. However, one could offer successive small challenge sets that children would not find difficult to swipe through to find “their” face. This approach maximizes both strength and usability. Thus, we commenced with challenge sets that contained six images for the two younger groups and increased the sets to contain nine 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, four- to five-year-old children should only have one target image to identify, while six- to seven-year-old children should identify two. The eight- to nine-year-old children should be able to remember four 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 do not resemble a child’s target image too closely (Renaud, 2009a). For the youngest group, it is important to choose appropriate distractors to eliminate confusion. We recommend using a tool such as the one that Karras et al. (2020) proposed to generate non-existent yet very real-looking faces to use as distractor images. Hence, faces of people that children could not possibly “know” would surround their target image. For the six- to seven-year-old age group, KidzPass uses doodles that researchers draw, which ensures that the distractors will differ from the ones that children draw and will eliminate confusion. For the generic images, one should avoid visual similarity (Hitch, Halliday, Schaafstal, & Schraagen, 1988), but this age group has a much greater ability to distinguish between images given their greater maturity.

Evaluation-related guidelines:

- Device: (refer to G1) Conduct evaluations using a tablet to minimize the impact of children’s technological naivety.
- Memorability: Test whether children can recognize their images after enrolling by returning to test their memory after a delay. 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 seven days (Brown & Scott, 1971; Reese, 1975), which we followed.
- Listening: (refer to G6) Allow children to express opinions throughout the evaluation and give them time to speak and express their opinions.

Finally, researchers need to conduct any KidzPass evaluation in an ethical manner. Thus, their institutions’ ethical review boards should approve their studies on KidzPass. Figure 2 depicts the framework and its configurable aspects depending on the target user group’s age. The first two studies that are shown in Figure 2 (i.e., age 4-5 and 6-7) were first reported in Stewart et al. (2020).

The research questions we explore in this investigation are:

RQ1: Can four- to five-year-old children successfully authenticate themselves using familiar faces in KidzPass?

RQ2: Can six- to seven-year-old children successfully authenticate themselves using self-drawn doodles in KidzPass?

RQ3: What qualities should generic images exhibit to make them suitable for KidzPass to use to authenticate eight- to nine-year-old children?

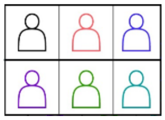
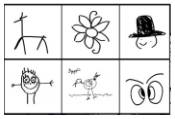
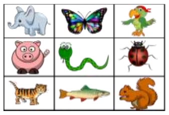
AGE	4-5	6-7	8-9
IDENTIFICATION			User Name
ACTION TO AUTHENTICATE	Recognize Face	Recognize Two Doodles	Recognize Four Objects
IMAGE TYPE	Familiar Faces	Hand-Drawn Doodles	Images Of Objects
IMAGE SOURCED	Provided by Parent	Drawn by Child	Randomly Allocated
CHALLENGE SET SIZE			
DISTRACTORS	Generated Faces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

Figure 2. The Configurable KidzPass Framework

4 KidzPass for Four- to Five-year-old Children: Using Familiar Faces

Obtaining authentication images: We asked parents to provide a photo of an adult whom their child found familiar but who did not pick them up from school. Such a photo maximized memorability for the child and minimized 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 they had chosen a particular image, we removed it 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 could play a game. If not, we gave them as many opportunities as they liked to try again.

Testing memorability: A week after enrolling, we 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 our research study. The primary researcher applied for and obtained an enhanced Disclosure Scotland check (https://disclosures.org.uk). We obtained signed consent from parents. A teacher was present during all interactions with the children. We gave children a sticker to thank them for their participation.

Methodology: Eight children (six males and two females) participated in this study.

First session (enrolling): During the first session, the children first registered by choosing an identification image. We then showed them how to choose "their" familiar face by swiping through successive challenge sets. Second, they logged in and played a child-appropriate game. Third, they expressed their opinions about KidzPass.

Second session (testing memorability): A week later, each child first logged in with their chosen animal identification image and "their" familiar face and played a child-appropriate game. Second, they expressed their opinions about KidzPass. We evaluated KidzPass's usability (i.e., its efficacy, efficiency, and satisfaction (ISO, 2018)).

4.1 Results

One child selected the wrong face during registration, while 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 we can understand since they could not read. On reflection, we should not have placed the registration button next to the login button, and we corrected this suboptimal design choice before the next evaluation. However, all three children recovered from their errors and logged in successfully. In both the first and second sessions, we recorded how long it took for the children to register and log in. Figure 3 depicts how long each child took. Note that these timings depended on the randomization algorithm so that a longer time could mean that the child had to swipe through more challenge sets before seeing “their” picture. However, they do provide 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 in two children due to their having to swipe through multiple challenge sets before they saw “their” face. We subsequently refined KidzPass to limit how many swipes children had to go through to avoid potential frustration.

4.2 Discussion

Even though we conducted the evaluation with only eight children, we found that the four- to five-year-old children could pick their animal image and log in successfully by identifying their familiar adult. We particularly noticed the children’s increased confidence during the second session. The timings we obtained do not reliably indicate efficiency because the login time depends on the randomization process that decides when the child’s familiar face appears. From the qualitative data gathered during the interviews with the children, we found the children preferred KidzPass to text-based passwords (Stewart et al., 2020).

In conclusion, we found that KidzPass proved effective for four- to five-year-old children. The children enjoyed using it. However, we acknowledge that their enthusiasm for the game likely cast a rosy glow over KidzPass itself, but the children certainly did not respond negatively when we asked them for their opinions. Although we did not test a text-based system in direct comparison, the children had used passwords in other contexts and expressed a preference for KidzPass.

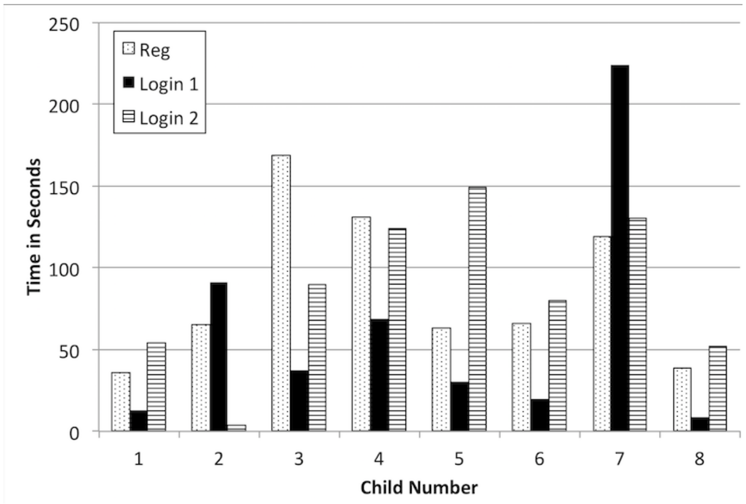


Figure 3. Registration and First and Second Login Times

5 KidzPass for Six- to Seven-year-old Children: Using Self-drawn Doodle Images

Obtaining authentication images: We provided the children with a template so that they could provide us with two doodles.

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

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 could play a game. If not, we gave them as many opportunities as they liked to try again.

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

Ethics: We followed the same procedure as for the previous KidzPass evaluation.

5.1 Methodology

We followed the same ethical approval process as for the four- to five-year-old children. In total, nine children (generally a year older than the children in the first study and in school) participated in the study.

First session (enrolling): The children first watched a video that explained how the system worked. Second, they registered by choosing an animal identification image. Third, they logged in by identifying their doodles and played a child-appropriate game.

Second session (testing memorability): A week later, the children first logged in with their chosen animal identification image and identified their two doodles, and then played a child-appropriate game. Next, they expressed their opinions about KidzPass.

5.2 Results

The animal-identification images proved the most popular application feature possibly due to popular animal-based films, television shows, and books that encourage young children to form a positive relationship with animals.

Two children had to authenticate twice at the first login, which happened again with two children at the second login. Selection inaccuracies mostly caused the failed login attempts, though one participant struggled to remember her animal identifier: She originally selected a bee as her username image but believed that her image was the frog. The frog had featured in the tutorial video as an example, which may explain why she mistook her image. After we realized that the frog in the tutorial video could confuse children, we removed the frog from selection to prevent any further confusion. We show how long the children took in the three stages in Figure 4. Once again, these timings depended on the randomization algorithm.

5.3 Discussion

Even though we conducted the evaluation with only nine children, we found that they could easily identify their animal image and log in successfully by identifying their hand-drawn doodles. Again, we particularly noticed the children's increased confidence during the second session. 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.

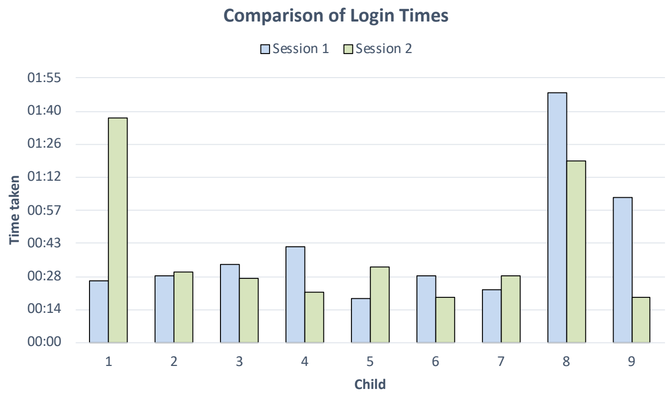


Figure 4. KidzPass Identification & Authentication Times (Second Study)

6 KidzPass for Eight- to Nine-year-old Children: Identifying Required Qualities of Generic Images

The images we used for KidzPass for younger children have proven efficacy in the authentication context (Brostoff & Sasse, 2000; Stewart et al., 2020). For eight- to nine-year-children, we used generic images in KidzPass to improve scalability and benefit from their greater maturity. Before we evaluated the mechanism with such children, we needed 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 eight- to ten-year-old children.

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 5 for the grids). We used challenge sets with nine rather than six images due to the children's greater maturity, and they needed to remember four images. We showed the images to the children's teacher to test their suitability in terms of understandability, and she considered them to be appropriate. We show the four grids in Figure 5.

First exposure to target images: The teacher, having welcomed everyone, started the lecture with our memory game. The teacher asked the children to focus on the digital board for a minute and not to speak during this minute. The teacher told them she would provide more information at the end of the lesson. Note that the teacher did not mention the need for the children to remember the images when she initially displayed the images. The teacher then displayed one animal, one car, one ship, and one building each for about five 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. Afterward, the lesson continued as originally planned.

Memorability test: We tested the immediate memorability using printed grids. Before the lecture, the teacher prepared four one-page image grids with randomly ordered images. At the end of the lesson, the teacher told the children that they would now return to the images they had seen when the lecture began. The teacher gave them four pages that contained images and instructed them to mark the image in the grid that they had seen before. The teacher asked them not to talk to one another during the task but rather to wait until everyone had completed it. They brought their pages to the teacher when they had completed the task. Note that the teacher distributed the grids in such a way that children who sat next to each other got differently ordered grids (just to make sure that they could not easily easy to see which image others marked). The teacher asked the children to select the correct images in the grids one hour and 15 minutes after first showing them the images to allow for sufficient time for forgetting to occur (Ebbinghaus, 1885).

Memorability test after seven days: A week later, the teacher distributed printed grids to the children again and asked them to mark the image they remembered from the previous week. The children were debriefed (i.e., that such an approach could be used in the future to log in to their computers rather than passwords). The teacher explained that, in this case, every child would get a different set of images to remember.

Ethics: The children's teacher conducted the study during an informatics lecture. We collected no personal data from or about the children. The teacher did not grade their performance and behavior during the study. As such, we did not need to secure ethical approval nor did we have to get permission from their parents.

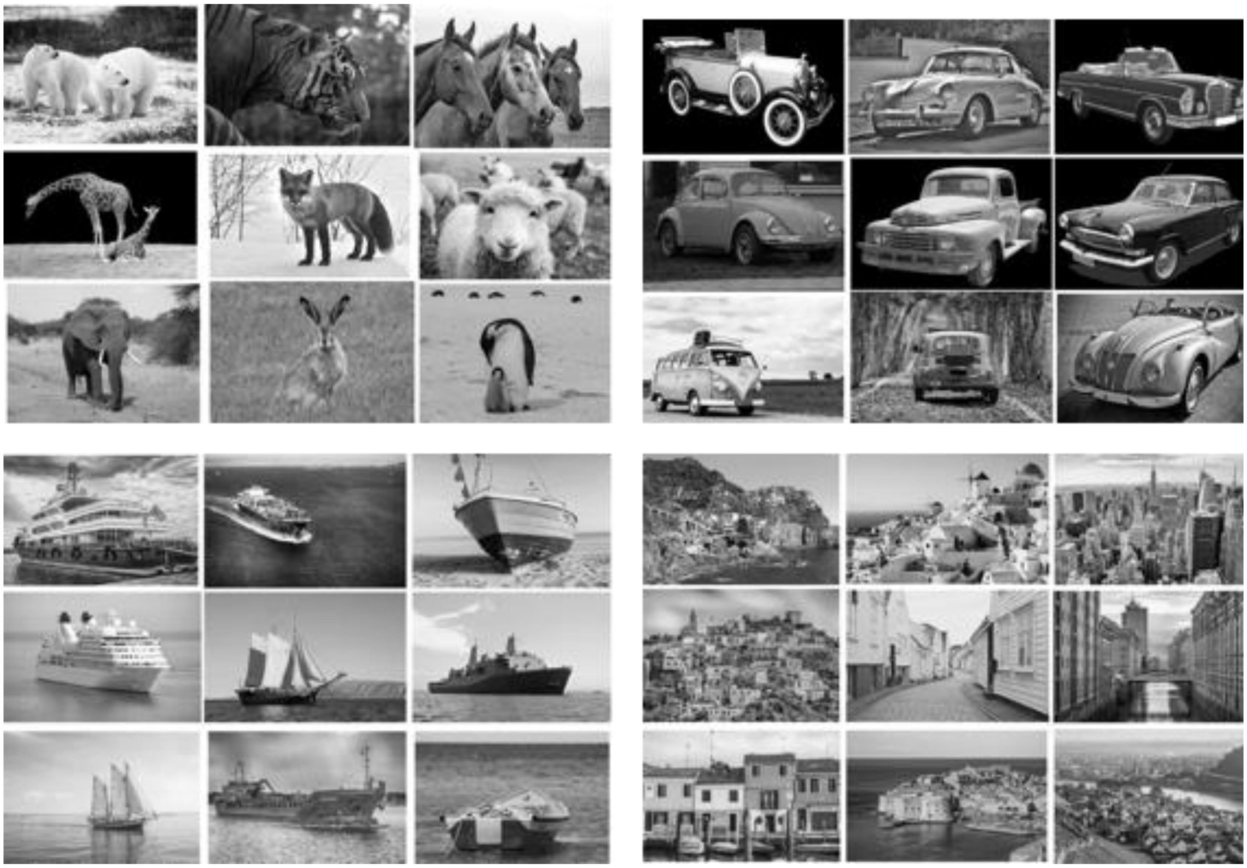


Figure 5. The Four Grids Used in the Third Study

6.1 Results

In total, 44 children participated. The teacher conducted the study in two classrooms: one with eight- to nine-year-old children (21 in total) and one with nine- and ten-year-old children (23 in total). We could conduct the second memorability test only in one class because the COVID-19 pandemic had closed schools. We conducted the test with an older group too to see whether the older group exhibited marked improvements in memorability.

Eight- to nine-year-old children: All children remembered the animal. One child selected the wrong car. The correct building was not selected by two children. Five children did not select the correct ship image. One child had issues with two image types, and six had issues with one image type. The remaining 14 children correctly identified all images in the grids. For this group, we could not collect data a week later.

Nine- to ten-year-old children: At the end of the lesson, all children got the animal, the car, and the ship correct. Three children had issues with the building. A week later, halfway through the informatics class, the children once again marked the image in the grids. Again, all remembered the animal, the car, and the ship. However, this time, five children had an issue remembering the building. Eighteen children got everything correct a week later.

7 Reflection

We had a positive experience evaluating KidzPass for the two younger age groups. Most children authenticated both the first and second time and seemed to enjoy interacting with the mechanism (and with the game). Hence, we can answer RQ1 and RQ2 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 (1985) argued that children's existing "knowledge base" influences how they acquire, retain, and retrieve information. As such, we should make sure that children have sufficient working knowledge of the images such that they can label them differently. Bjorklund and Zaken-Greenberg (1981) argued that children construct image taxonomies in their minds such that they store images that belong to the same category together, which 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, they create make identification errors.

Nine-year-old children possibly lack familiarity with the individual names for complex buildings and so could not uniquely label the "secret" image. They would merely call it a building rather than a "beach house" or a "Venetian building".

Ability to label: We believe it realistic to expect older children to be able to memorize these images given that the ability to remember images improves with age (Cycowicz, Friedman, Snodgrass, & Duff, 2001). However, and related to the previous point, Hitch and Halliday (1983) suggested that two working memory stores exist: 1) the articulatory loop, involved in subvocal rehearsal, and 2) the visuo-spatial scratch-pad, involved in imagery. The authors argued 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). We find this argument interesting because it suggests that the ease with which older children can assign labels to images will impact how well they can remember images.

Reese (1975) also found that younger preschoolers relied on visual memory to recognize images, while older preschoolers began to use image labels to reconstruct images by relying on their verbal memory. Once again, these findings confirm the need for children to be able to assign a label to a generic image in order to encode and retain it in their memory so that they can retrieve it 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 with faces (Gobbini & Haxby, 2007), while the second relied on action planning memory (Knoblich & Prinz, 2001), which children imprint in their memory as they draw a doodle. In these cases, ease of labeling becomes less important.

Distractor choice: KidzPass for the younger children used personalized images: familiar faces and doodles—all images in the challenge sets came from the same category. In hindsight, we did not have to use this strategy for generic images as we did. It might be that, when one uses generic images, one should use distractor images from completely different categories to avoid the labeling difficulties the children experienced. So, for example, if a ship represents a child's target image, the distractor images could be a building, a toy, a bed, and so on.

Image content: One guideline for designing graphical authentication states that images should contain a single object with a clear background to simplify labeling (Renaud, 2009a). The building category demonstrates this guideline's importance. All the images show multiple buildings, which do not lend themselves to easy labeling. On the other hand, the children could easily label the animals. Each image shows an easily identified animal, and children learn animal names at an early age.

Finally, we note that the teacher facilitated the memory check by handing out paper copies of the grids in grayscale (due to resource constraints at the school). Thus, the children may have more easily distinguished the images that they struggled to remember from other images if they had been printed in color since color provides an extra cue.

7.1 Required Qualities of Generic Images

To answer RQ3, we suggest that, when using generic images in KidzPass to authenticate children over eight years old should display several qualities that we discuss below.

(Q1) Understandability: One should construct challenge sets from images that substantively differ from each other (Fioravanti et al., 1995; Duncan et al., 1994; Murphy-Berman et al., 1986).

(Q2) Ease of labeling: One should ensure that the target users have the vocabulary to label each image uniquely. This guideline applies even to adults. One author could not identify more than two cars that the car set depicted. To gauge what vocabulary one can expect a child oat any age to have, one can look at children's books (Zwiers & Morrissette, 2013).

(Q3) Image content: An 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 depict a particular city (which a young child would not likely identify correctly). It also includes a river and what looks like a church. Consider that children saw this image and chose the label “river”. Seeing the grid a week later, they could easily think that they had previously seen the image directly above that one, which one could also arguably label as “river”. If they picked out the steeple on one of the other pictures that show a steeple and then saw the entire grid, they would see two pictures with steeples. Hence, one has to choose graphical authentication images with great care to avoid confusion.

(Q4) Use colored images because it can enhance distinctions between images.

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

7.2 Challenges and Limitations

(C1) Recruitment difficulties: The small sample size undeniably inhibited quantitative analysis. We could not contain a larger sample size due to difficulties in recruiting participants (Stewart et al., 2020). In the first study, we realized that the difficulty emerged because we asked busy parents to provide a photo of someone familiar to their child. We had provided them with comprehensive instructions. In retrospect, this request created a barrier to participation. For KidzPass for six- to seven-year-old children, we switched to asking the children themselves to draw images, which removed the barrier. Parents happily permitted 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. As a result, they understandably limit the number of requests they agree to.

(C2) Time-intensive evaluation: We could not feasibly conduct initial KidzPass tests online because we wanted to observe children 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 decision proved wise, and we advise other researchers to follow it. However, it did make the evaluation more time-consuming.

(C3) Easing transition to KidzPass: System developers use passwords because they know users are familiar with them. We have argued that the password does not represent a suitable option for authenticating young children. KidzPass undoubtedly has benefits for younger computer users. However, to encourage developers to adopt it, we will have to make the transition to KidzPass as painless and inexpensive as possible. Thus, we would make the software free so developers do not incur any additional monetary outlay. It would also be helpful to provide KidzPass as a plug-and-play component, which future research could examine.

8 Age-appropriate Authentication-design Principles

In designing a graphical authentication mechanism, one needs to keep children’s capabilities in mind and 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 efforts to design and evaluate graphical authentication mechanisms for primary school children. We present two kinds of design principles: 1) ethical ones, and 2) technical ones. We ground them as we show in Figure 6.

8.1 Ethical Principles

The United Kingdom’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 efforts to design and evaluate age-appropriate authentication mechanisms in an ethical manner. In Table 1, we contextualize the provided age-appropriate design principles to the graphical authentication context and place the ICO’s principles in the leftmost column. Researchers should seek approval from their institutions’ ethical review boards before commencing any evaluations with children to demonstrate how they align with the ethical principles.

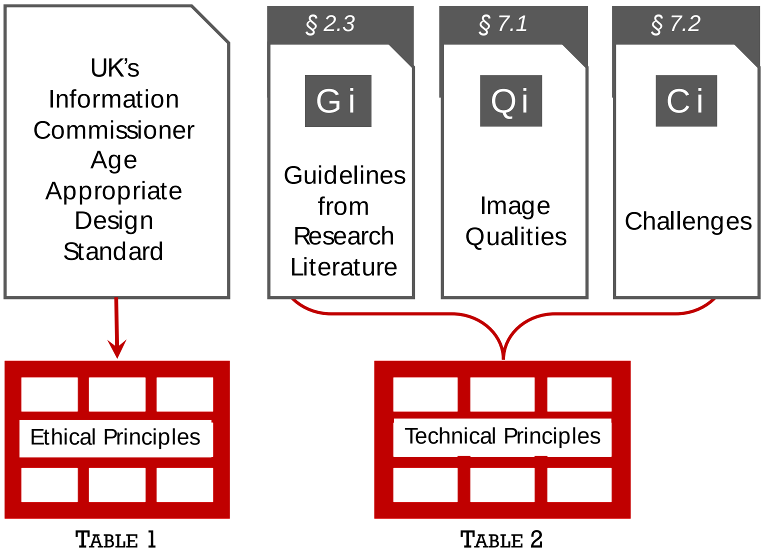


Figure 6. Sources of the Ethical and Technical Principles

Table 1. Ethical Principles for Designing and Evaluating Age-appropriate Authentication Mechanisms

Principle	Design	Evaluation
Children's best interests	Design the mechanism in line with children's capabilities.	See Figure 2 and Table 2.
Data-protection impact assessment	Develop a data-protection impact assessment (DPIA).	Researchers should give children and parents the chance to have a say in how they will use their data to help build trust and improve their knowledge about child-specific needs, concerns, and expectations.
Age-appropriate application	User incentives play an important role in providing a desire for young children to want to engage with the system. Reward children for using KidzPass by letting them play a game.	User testing represents the only way researchers can determine the designed system's suitability for the intended user population.
Transparency	The interface of the authentication mechanism should always represent its current internal state to minimize the gulf between evaluation and execution. For example, prominently display visible cues for children so that they know what actions they should take and what the system will do as a consequence.	Children can assent to participate in a research study (Weithorn, 1983). Obtain this consent. Researchers should inform them that they can stop at any time. Use pseudonyms in writing up the research (Curtin, 2001).
Detrimental data use	Do not use children's data for any other purpose than authentication.	Researchers should ensure that they inform parents about how they will use their children's data that they collect for evaluation purposes. Take no photographs without parental consent.
Policies and community standards	In the European Union, researchers need to ensure that they adhere to GDPR standards. They should only collect data that they need for the authentication and make sure that they either encrypt or hash child-provided data that they store to ensure that no sensitive information the child potentially entered can leak in plain text. If they cannot encrypt or hash data, they should ensure that they identify which data could leak in case a cyber-incident occurs.	Obtain ethical approval and signed consent from parents and ensure that they know exactly what the evaluation involves.

Table 1. Ethical Principles for Designing and Evaluating Age-appropriate Authentication Mechanisms

Data minimization	Collect only the information needed to authenticate children.	Researchers should only collect data that they need to test the authentication mechanism's usability.
Data sharing	Only share a child's data with explicit consent from the parents.	Provide data sharing information if the children are old enough to understand this.
Nudge techniques	Only use nudges for children's benefit, not a platform's.	Researchers must explain the mechanisms behind the nudge and its anticipated influence on parents and obtain permission from them to deploy the nudge with their child(ren).
Online tools	Uphold children's rights under the GDPR (European Union, 2018) and ensure that parents can satisfy themselves about this issue 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 latter's data and exercise their GDPR rights in this respect. Ensure that the child knows about their rights to their personal data before participating in an evaluation.

8.2 Technical Principles

The technical design principles we present in Table 2 cover efforts to design and evaluate age-appropriate authentication mechanisms developed for research purposes. Using graphical authentication as a password alternative addresses G4 and G5 (see Section 2.3). To date, because researchers have conducted only a few empirical evaluations, we do not yet know how to prioritize these guidelines nor what ones to classify as essential or simply good to follow. Future research could address this topic.

Table 2. Technical Guidelines for Designing and Evaluating age-appropriate Authentication Mechanisms

Principle	Design	Evaluation
Use a tablet (G1, G4)	This principle 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, maximize memorability and ease of use by using familiar images. For older children, one can use generic images but only when chosen with care. Ensure that the target user group can uniquely label the images you choose (i.e., that an average child of that age can perform the vocabulary and categorization).	Memorability of images ought to be confirmed in a pilot study with the target demographic.
Age-appropriate literacy requirements (G2)	Children in the four- to five-year-old 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 the 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 (in accordance with ethical constraints in Table 1).	
Hear children's voices (G6)	We need to hear children's voices and respect their opinions and perceptions of the authentication mechanisms we design for them. In the second study, we used a questionnaire with questions and emoticons that we 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.

Table 2. Technical Guidelines for Designing and Evaluating age-appropriate Authentication Mechanisms

There are no shortcuts (C2)	It will take researchers much longer to evaluate these mechanisms with children than with adults. Expect that and do not try to speed things up. We did measure how long it took to authenticate but such measurements depend on the image randomization process, which makes them unreliable signifiers of usability. The design specifically chose to randomize 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)	We developed KidzPass 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 and not subject to copyright. We used such images to ensure that adopters could use them without financial limitations.	Ensure that all images are free to use and that software subscriptions are not required.
Note: the leftmost column emerged from our studies. "G#" refers to guidelines that we list in Section 2.3, "Q#" refers to image qualities that we derived in Section 7.1, and "C#" refers to challenges that we mention in Section 7.2.		

9 Conclusion and Future Work

We developed KidzPass, a framework for configurable age-appropriate graphical authentication mechanisms, specifically to authenticate young children. We conducted two qualitative studies to evaluate KidzPass using personalized images. We and our children participants found both studies very rewarding. We found that the children could log in successfully and enjoyed participating.

However, we realized that the mechanism would not scale sufficiently to support wide-ranging deployment mostly because we used personalized image types. Thus, we conducted a third study with 44 children to test whether they could remember less personalized images. Once again, we found the need to consider the images that these kinds of authentication mechanisms use to maximize memorability and suitability.

Based on our experience conducting our studies, we believe it important 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 United Kingdom's age-appropriate authentication design standard and technical principles to inform efforts to design and evaluate these age-appropriate graphical authentication mechanisms.

In the future, if we want to deploy KidzPass outside a research environment, we need to address the following:

- **Facilitating existing authentication replacement**: Software in schools use passwords. While educational authorities might be well disposed towards replacing passwords 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 replacing passwords 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 practices and to help them to convey these principles to the children in their care. We have already seen initial steps in this direction (see https://cybersquad.uk).
- **Accessible authentication for young children**: Clearly, only sighted children can use KidzPass. Thus, we need alternatives to passwords that can accommodate individuals in this demographic with vision difficulties as well.

Acknowledgments

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, E., Petrie, H., & Renaud, K. (2020). Kidsdoodlepass: An exploratory study of an authentication mechanism for young children. In *Proceedings of the International Symposium on Human Aspects of Information Security & Assurance*.

Anagnostaki, L., Wright, M. J., & Papathanasiou, A. (2013). *Secrets and disclosures: How young children handle secrets*. *The Journal of Genetic Psychology*, 174(3), 316–334.

Assal, H., Imran, A., & Chiasson, S. (2018). An exploration of graphical password authentication for children. *International Journal of Child-Computer Interaction*, *18*, 37-46.

Barrett, L. F. (2017). *How emotions are made: The secret life of the brain*. Harcourt, NY: Houghton Mifflin.

Biddle, R., Chiasson, S., & van Oorschot, P. C. (2012). *Graphical passwords: Learning from the first twelve years*. ACM Computing Surveys, *44*(4), 1-41.

Bjorklund, D. F., & Zaken-Greenberg, F. (1981). The effects of differences in classification style on preschool children's memory. *Child Development*, *52*(3), 888-894.

Bosse, M.-L., & 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, S., & Sasse, M. A. (2000). Are passfaces more usable than passwords? A field trial investigation. In S. McDonald, Y. Waern, & G. Cockton (Eds.), *People and computers XIV—usability or else!* London, UK: Springer.

Brown, A. L., & Campione, J. C. (1972). Recognition memory for perceptually similar pictures in preschool children. *Journal of Experimental Psychology*, *95*(1), 55-62.

Brown, A. L., & Scott, M. S. (1971). Recognition memory for pictures in preschool children. *Journal of Experimental Child Psychology*, *11*(3), 401-412.

Cain, A. A., & Still, J. D. (2018). Usability comparison of over-the-shoulder attack resistant authentication schemes. *Journal of Usability Studies*, *13*(4), 196-219.

Chiasson, S., Van Oorschot, P. C., & Biddle, R. (2007). Graphical password authentication using cued click points. In *Proceedings of the European Symposium on Research in Computer Security*.

ChildTrends. (2018). *Home computer access and Internet use*. Retrieved from https://www.childtrends.org/indicators/home-computer

Choong, Y.-Y., Theofanos, M., Renaud, K., & Prior, S. (2019). Case study—exploring children's password knowledge and practices. In *Proceedings of the Workshop on Usable Security.*

Chowdhury, S., Poet, R., & Mackenzie, L. (2013). Exploring the guessability of image passwords using verbal descriptions. In *Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications.*

Chu, X., Sun, H., & Chen, Z. (2020). Passpage: Graphical password authentication scheme based on Web browsing records. In *Proceedings of the International Conference on Financial Cryptography and Data Security.*

Coggins, P. E., III. (2013). *Implications of what children know about computer passwords*. *Computers in the Schools*, *30*(3), 282-293.

Cordon, I. M., Melinder, A. M., Goodman, G. S., & 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, D. A., Jacobus, K. A., & Leonard, S. D. (1969). Recognition memory of preschool children for pictures and words. *Psychonomic Science*, *16*(4), 192-193.

Cowan, N., AuBuchon, A. M., Gilchrist, A. L., Ricker, T. J., & Saults, J. S. (2011). Age differences in visual working memory capacity: Not based on encoding limitations. *Developmental Science*, *14*(5), 1066-1074.

Curtin, C. (2001). Eliciting children's voices in qualitative research. *American Journal of Occupational Therapy*, *55*(3), 295-302.

Cycowicz, Y. M., Friedman, D., Snodgrass, J. G., & Duff, M. (2001). Recognition and source memory for pictures in children and adults. *Neuropsychologia*, *39*(3), 255-267.

Darbanian, E., & Fard, G. D. (2015). A graphical password against spyware and shoulder-surfing attacks. In *Proceedings of the International Symposium on Computer Science and Software Engineering.*

de Haan, M., Johnson, M. H., Maurer, D., & 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, R., & Perrig, A. (2000). Deja vu: A user study using images for authentication. In *Proceedings of the USENIX Security Symposium.*

Duncan, J., Ward, R., & Shapiro, K. (1994). Direct measurement of attentional dwell time in human vision. *Nature*, *369*(6478), 313-315.

Dunphy, P., Nicholson, J., & Olivier, P. (2008). Securing passfaces for description. In *Proceedings of the 4th Symposium on Usable Privacy and Security*.

Ebbinghaus, H. (1885). *Uber das gedächtnis: Untersuchungen zur experimentellen psychologie*. Leipzig: Duncker & Humblot.

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). *General data protection regulation GDPR*. Retrieved from https://gdpr-info.eu/

Fernandes, M. A., Wammes, J. D., & Meade, M. E. (2018). The surprisingly powerful influence of drawing on memory. *Current Directions in Psychological Science*, *27*(5), 302-308.

Filan, G., & Sullivan, H. (1980). Effects of induced memory strategies on children's memory for pictures and words. In *Proceedings of the Annual Educational Research Association Annual Convention*.

Fioravanti, F., Inchingolo, P., Pensiero, S., & Spanio, M. (1995). Saccadic eye movement conjugation in children. *Vision Research*, *35*(23-24), 3217-3228.

Frey, A., & 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, S. E. (1999). Cognitive approaches to the development of short-term memory. *Trends in Cognitive Sciences*, *3*(11), 410-419.

Gobbini, M. I., & Haxby, J. V. (2007). Neural systems for recognition of familiar faces. *Neuropsychologia*, *45*(1), 32-41.

Henson, R., Shallice, T., & Dolan, R. (2000). Neuroimaging evidence for dissociable forms of repetition priming. *Science*, *287*(5456), 1269-1272.

Herley, C., & van Oorschot, P. (2012). *A research agenda acknowledging the persistence of passwords. IEEE Security & Privacy*, *10*(1), 28-36.

Hitch, G., & Halliday, M. (1983). Working memory in children. *Philosophical Transactions of the Royal Society of London B: Biological Sciences*, *302*(1110), 325-340.

Hitch, G. J., Halliday, S., Schaafstal, A. M., & Schraagen, J. M. C. (1988). Visual working memory in young children. *Memory & Cognition*, *16*(2), 120-132.

Hlywa, M., Biddle, R., & Patrick, A. S. (2011). Facing the facts about image type in recognition-based graphical passwords. In *Proceedings of the Annual Computer Security Applications Conference*.

Information Commissioner's Office. (2020). *Age appropriate design: A code of practice for online services.* Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protectionthemes/age-appropriate-design-a-code-of-practice-for-online-services/.

ISO. (2018). *Ergonomics of human-system interaction*—part *11: Usability: Definitions and concepts.* Retrieved from https://www.iso.org/standard/63500.html

Jenkins, R., McLachlan, J. L., & Renaud, K. (2014). *Facelock: Familiarity-based graphical authentication*. *PeerJ*, *2*, e444.

Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., & Rubin, A. D. (1999). The design and analysis of graphical passwords. In *Proceedings of the 8th USENIX Security Symposium.*

Karras, T., Laine, S., Aittala, M., Hellsten, J., Lehtinen, J., & Aila, T. (2020). Analyzing and Improving the image quality of StyleGAN. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*.

King, M. M. (1991). Rebus passwords. In *Proceedings of the Annual Computer Security Applications Conference.*

Knoblich, G., & Prinz, W. (2001). *Recognition of self-generated actions from kinematic displays of drawing. Journal of Experimental Psychology: Human Perception and Performance*, *27*(2), 456-465.

Li, Z., Sun, Q., Lian, Y., & Giusto, D. D. (2005). An association-based graphical password design resistant to shoulder-surfing attack. In *Proceedings of the IEEE International Conference on Multimedia and Expo*.

Marques, J. F. (2007). Unlearning: The hardest lesson of all. *Performance Improvement*, *46*(1), 5-6.

Mayer, P. (2019). *Secure and usable user authentication* (doctoral thesis). Karlsruhe Institute of Technology, Karlsruhe, Germany.

Mayer, P., Volkamer, M., & Kauer, M. (2014). Authentication schemes—comparison and effective password spaces. In *Proceedings of the International Conference on Information System Security*.

Mendori, T., Kubouchi, M., Okada, M., & Shimizu, A. (2002). Password input interface suitable for primary school children. In *Proceedings of the International Conference on Computers in Education*.

Mihajlov, M., & Jerman-Blazic, B. (2018). Eye tracking graphical passwords. In P. Magnaghi-Delfino & T.. Norando (Ed.), *Advances in intelligent systems and computing* (pp. 37-44), San Diego, CA: Springer.

Moore, T., McArthur, M., & 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, E. F. (1915). Experimental studies in recall and recognition. *The American Journal of Psychology*, *26*(2), 217-228.

Munoz, D., Broughton, J., Goldring, J., & Armstrong, I. (1998). Age-related performance of human subjects on saccadic eye movement tasks. *Experimental Brain Research*, *121*(4), 391-400.

Murphy-Berman, V., Rosill, J., & Wright, G. (1986). Measuring children's attention span: A microcomputer assessment technique. *The Journal of Educational Research*, *80*(1), 23-28.

Nelson, D. L., Reed, V. S., & John R, W. (1976). Pictorial superiority effect. *Journal of Experimental Psychology: Human Learning and Memory*, *2*, 523-528.

Ornstein, P. A. & Naus, M. J. (1985). Effects of the knowledge base on children's memory strategies. *Advances in Child Development and Behavior*, *19*, 113-148.

Paivio, A., & Csapo, K. (1973). Picture superiority in free recall: Imagery or dual coding? *Cognitive Psychology*, *5*(2), 176-206.

Paivio, A., Rogers, T. B., & Smythe, P. C. (1968). Why are pictures easier to recall than words? *Psychonomic Science*, *11*, 137-138.

Peskin, J., & 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, S., & Renaud, K. (2020). Age-appropriate password "best practice" ontologies for early educators and parents*. International Journal of Child-Computer Interaction*.

Ratakonda, D. K., French, T., & 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*.

Read, J. C., & Cassidy, B. (2012). Designing textual password systems for children. In *Proceedings of the 11th International Conference on Interaction Design and Children.*

Reese, H. W. (1975). Verbal effects in children's visual recognition memory. *Child Development*, *46*(2), 400-407.

Renaud, K. (2009a). Guidelines for designing graphical authentication mechanism interfaces. *International Journal of Information and Computer Security*, *3*(1), 60-85.

Renaud, K. (2009b). Web authentication using Mikon images. In *Proceedings of the World Congress on Privacy, Security, Trust and the Management of e-Business.*

Renaud, K., & Maguire, J. (2009). Armchair authentication. In *Proceedings of the 23rd British BCS Human Computer Interaction Group Annual Conference on People and Computers.*

Renaud, K., Mayer, P., Volkamer, M., & Maguire, J. (2013). Are graphical authentication mechanisms as strong as passwords? In *Proceedings of the Federated Conference on Computer Science and Information Systems*.

Shammee, T. I., Akter, T., Mou, M., Chowdhury, F., & Ferdous, M. S. (2020). A systematic literature review of graphical password schemes. *Journal of Computing Sciences and Engineering*, *14*, 163-185.

Siegler, R. (2013). *Children's thinking: What develops?* Hillsdale, NJ: Psychology Press.

Sowell, E. R., Thompson, P. M., Leonard, C. M., Welcome, S. E., Kan, E., & Toga, A. W. (2004). Longitudinal mapping of cortical thickness and brain growth in normal children. *Journal of Neuroscience*, *24*(38), 8223-8231.

Stewart, M., Campbell, M., Renaud, K., & Prior, S. (2020). Kidzpass: Authenticating pre-literate children. *Proceedings of the Dewald Roode Workshop on Information Systems Security Research.*

Suo, X., Zhu, Y., & Owen, G. S. (2005). Graphical passwords: A survey. In *Proceedings of the Annual Computer Security Applications Conference*.

Tversky, B. (1973). Encoding processes in recognition and recall. *Cognitive Psychology*, *5*(3), 275-287.

Weinshall, D. (2006). Cognitive authentication schemes safe against spyware. In *Proceedings of the Symposium on Security and Privacy.*

Weithorn, L. A. (1983). Involving children in decisions affecting their own welfare. In G. B. Melton, G. P. Koocher, & M. J. Saks (Eds.), *Children's competence to consent*. Boston, MA: Springer.

Williams, A. D. (2015). *The development of a music program to improve the attention span of school-aged children* (master's thesis). Minneapolis, MN: Capella University.

Yan, J. J., Blackwell, A. F., Anderson, R. J., & Grant, A. (2004). Password memorability and security: Empirical results. *IEEE Security & Privacy*, *2*(5), 25-31.

Yang, G. (2017).循环 Passpositions: A secure and user-friendly graphical password scheme. In *Proceedings of the 4th International Conference on Computer Applications and Information Processing Technology.*

Zhang-Kennedy, L., Mekhail, C., Abdelaziz, Y., & 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*.

Zimmermann, V., & 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, M., & Morrissette, P. J. (2013). *Effective interviewing of children: A comprehensive guide for counselors and human service workers.* Ann Arbor, ML: Taylor & Francis.

About the Authors

Karen Renaud does research on all aspects of Human-Centred Security and Privacy. She is a Fulbrighter and Visiting Professor at Rhodes University in Grahamstown, South Africa and Abertay University in Dundee, Scotland and also Professor Extraordinaire at the University of South Africa. She is particularly interested in improving the interface where humans and security/privacy meet, which includes understanding the problems people experience and developing interventions to improve them. She was successfully nominated as KIT International Excellence Fellow for 2021.

Melanie Volkamer is a Full professor at KIT in the Department of Economics and Management. She leads the SECUSO research group. From August 2016 until March 2018, she was a Professor (Kooperationsprofessur) at the Department of Computer Science of Technische Universität Darmstadt Germany). From December 2015 to December 2018, she was appointed a Full Professor for Usable Privacy and Security at Karlstad University (Sweden). Previously, she was an Assistant Professor at TU Darmstadt. She has been heading the research group “SECUSO—Security, Usability and Society” since 2011. From 1 May to 31 August of 2011, she worked as a visiting researcher at CMU/CUPS.

Peter Mayer is a postdoctoral researcher in the SECUSO Research Group at Karlsruhe Institute of Technology. His research focuses on security awareness and education, usable authentication, and email security. Having graduated from Technische Universität Darmstadt with a Master’s degree in IT-Security as well as a Master’s degree in computer science with application subject “Biological Psychology” in 2014, he defended his PhD thesis on “Secure and Usable User Authentication” at Karlsruhe Institute of Technology in November 2019. He currently holds the roles of coordinator and co-speaker of the “Human and Societal Factors” research group in the Helmholtz Association funded subtopic “Engineering Secure Systems” at KIT.

Rüdiger Grimm was Professor for IT Risk Management at the Universities of Ilmenau and Koblenz 2000-2015. After retirement, he is continuing research, teaching and consulting in his old Fraunhofer Institute for Secure IT (SIT). Additionally, he is teaching usage of Computers, the Internet, and email to primary school pupils aged 8 to 10.

Transactions on Human – Computer Interaction