A PARENT - CHILD PASSWORD MANAGER

by
Kalpana Hundlani

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

MASTER OF SCIENCE

School of Computer Science

at

CARLETON UNIVERSITY

Ottawa, Ontario
September, 2016

Abstract

Many studies reflect that today's younger generation spends a considerable amount of time online whether for doing their homework or playing games. However, the authentication schemes for this user group has received negligible attention. When exploring alternate authentication mechanisms for children, we decided to reduce the password burden and involve parents in the authentication decision. We chose to explore whether a parent-child password manager was a good choice for achieving this goal.

We started with our 'Keep A Secret' prototype, a parent-managed password manager for children. On the next iteration, we designed 'KinderSurf', a parental consent mechanism based on the OpenID concept. We conducted two user studies for evaluating the prototypes. These user studies revealed areas for improvements, but overall both parents and children like the idea of using parental consent to log in.

Acknowledgements

"Tell me and I forgot, teach me and I may remember, involve me and I learn."'

-Benjamin Franklin.

Over the span of years, I have learnt something new every day. I would like to thank many wonderful people, who made this experience possible.

First and foremost, I would like to express my sincere gratitude to my supervisor Sonia Chiasson, for believing in me and being my guiding light throughout. Sonia, you always bring out the best in my work and constantly motivate me to perform better. Thank you for your guidance, support and patience. This research would not be possible without you. I am glad I had you as my mentor.

I would also like to thank the members of my committee, Timothy Lethbridge, Audrey Girouard, and Olga Baysal for their time, perspectives and constructive feedback that helped me improve this dissertation.

I would also like to thank Bluink Inc. for their collaboration in development of KinderSurf. Also, thanks to NSERC for funding this research.

Thanks to my colleagues in the Carleton Human Oriented Research in Usable Security research group who have helped me with experiments, presentations, and offered valuable feedback throughout the process. Their pointers and advice have always assisted me in achieving my goals.

I would also like to thank my family and friends for all their love and support. Special thanks to my parents and my brother for believing in me and letting me pursue my dreams despite all odds. Also, thanks to my friend Aditi for proofreading my thesis.

Lastly, I would like to thank everyone who has been a part of this journey of mine.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Motivation

Current authentication schemes are designed primarily with adults in mind; and have their own drawbacks [10]. The password problem [93] is characterized by usability issues related memorability. Despite the password problem, passwords are here to stay [10]. In response, users resort to coping strategies like re-using passwords, using simple easy-to-guess passwords, and writing them down in insecure locations. It is hard even for adults for protect themselves in the digital world, where phishing and identity theft occurrences are so common.

Children are one of the significantly growing users group of the internet, and are surrounded by digital devices from a very early age [32]. Media Smarts recently conducted survey [77] of 5,436 young Canadians and claimed that "Almost every student we surveyed (99%) has access to the internet outside of school, from a variety of (mostly portable) platforms and devices.". Multiple other studies show that today's younger generation spends a considerable amount of time online [2, 19, 46, 76, 80], whether for doing their homework or playing games. It is suggested that children should be made aware of the risks involved in being online and how to be safe [32, 67]. Children differ from adults in terms of skills, preferences and online literacy [7, 12, 62], so tools and protection mechanisms designed for adults are not necessarily appropriate.

However, the subject of child authentication has received very little attention. There is sparse research on assessing children's performance and preferences for authentication [37, 63] and few attempts to design child-friendly alternatives [50, 86]. In order to protect children, the major focus of the existing research has remained on monitoring tools [14, 17, 25, 27].

1.2 Research Direction

Our research focuses on user authentication for children and the main research question is:

> *"How do we simplify the authentication process for children while maintaining security?"*

Our initial exploration of the literature and available tools revealed that few alternatives exist. In an effort to minimize the password burden, we explore ways to simplify the password process for children. Password managers and OpenID were the apt choices for achieving this goal given that both reduce the number of passwords that a user has to remember. We also explore adding some customizable parental oversight to increase security for children.

As we explored alternative authentication schemes, we decided to explore the feasibility of a parent-child password manager. Our initial prototype transferred the burden of managing passwords on to adults but we found that this was not sufficient. As the research progressed, we iteratively re-designed our prototype. The improved prototype (KinderSurf), involved parents in authentication decisions as well as achieved password reduction.

Currently, the design is focused on children logging on to websites. The design ideas explored in this thesis could potentially be extended to other scenarios such as mobile apps or parental oversight of non-authenticated websites. However, this is beyond the scope of this thesis.

1.3 Contribution

The primary contribution of this thesis is the design and evaluation of an alternative mechanism for child-authentication. The major contributions are summarized below.

- We researched existing authentication schemes for children and realised that few child-specific options were available. Also, we found that children have little understanding of how to protect themselves on the internet. We thought of involving parents to aid children in the decision-making process and proposed the idea of a parent-child password manager.

- Based on our novel concept, we designed and developed two prototypes in an iterative process. We kept in mind the user group and tried to create an interface that is easy for children to understand and use. As part of the iterative process, our new prototype accommodated new features, user interface and protocol improvements, and participants' preferences.

- We conducted two users studies evaluating the prototype, involving both parents and children. We recruited participants, evaluated their task performances, analyzed their feedback, and took into consideration their needs and preferences during our redesigns. Based on these findings, we can say that both parents and children liked the concept of involving parents in the authentication process. Parents also liked the features allowing them some control over which sites children visit and when they visit.

1.4 Relationship with Bluink

This research is a joint project between our Carleton research team and Bluink [1], a local Ottawa technology company. It is funded by an NSERC Engage grant which is intended to foster collaboration between academic researchers and industry.

We initially explored our research idea independently. We added Bluink as a collaborator in the redesign phase of our prototype. We shared similar interest and complementary skills, based on which we distributed our responsibilities.

We were responsible for the user interface of the 'KinderSurf' app. We designed the interface and interaction flow of the prototype based on outcomes from the previous study, and Bluink's technology. We also developed the user interface prototype for carrying out user-testing. We continue to work with Bluink on developing a fully functional KinderSurf app as per the discoveries from our second study. We will eventually perform user-testing with a wider audience outside of the lab environment.

Bluink is responsible for the implementation and deployment of the KinderSurf app, as an adaptation to their original OpenID infrastructure. So far, they have

[1] `http://www.bluink.ca/`

developed the app's authentication mechanism linking parent devices and child accounts, and the framework for using the OpenID protocol. They have implemented the push notifications feature, that enables parents to remotely authorize child login requests. The implementation is currently on-going.

1.5 Thesis Outline

The remainder of the thesis is organised as follows:

- *Chapter 2* reflects the existing research done on relevant topics like authentication, passwords, password managers, OpenID and online security for children.
- *Chapter 3* describes the user interface and interaction of the low-fidelity prototype. It elaborates on our user-testing protocols and offers outcomes of our first user study.
- *Chapter 4* presents the design details of the KinderSurf app. The interface was based on insights from the previous study and Bluink's technology.
- *Chapter 5* covers the second user study and evaluation of the improved prototype. It discusses the study methodology and results.
- *Chapter 6* summarizes the research, discusses areas of improvements, and indicates future research directions.

Chapter 2

Background

This chapter provides an overview of existing work in the field of authentication, child authentication, password managers and OpenID.

2.1 Authentication

For computer systems, authentication consists of identification, user authentication and authorization [65]. Identification is the process where the user claims an identity. User Authentication is the process of verifying the claimed identity with evidence. Authorization is providing access rights to the approved users and denying them otherwise. Usually, authentication mechanisms have identification followed by verification, however sometimes they can operate as one step [71].

Authentication can be briefly categorized as follows [71]:

- Knowledge based: This technique refers to validating based on something a user knows. Examples include passwords, PINs, pattern, and graphical passwords [8, 15]. In all of these, the user answers a predefined secret question. This technique is easy to implement and inexpensive, but also relatively easy to compromise [57]. Among all authentication options, text passwords are the most common choice, despite usability and security issues [65, 96].

- Token based: This technique refers to validating based on something a user has. Examples include one time password generators or physical tokens like a phone or smart cards. This authentication requires the user to carry the physical entity and present it for authentication. However, since tokens can be lost or stolen, it is easy to compromise this authentication technique [57].

- Biometric: This technique refers to validating a user's identity based on their physical and behavioural characteristics. Examples of physical characteristics

used as biometrics include face, retina or fingerprint scans, while examples of behavioural biometrics include typing rhythm, gestures, and voice recognition. Biometric authentication is rapidly becoming part of our daily life and is perceived by users as one of the most secure methods [5]. However as it depends on one unique feature of your appearance or behaviour, if that feature changes due to any reason, then it is difficuilt to gain access or replace the authenticating feature [57].

All authentication mechanisms have their strengths and weaknesses [20, 33, 57]. In order to overcome the weakness of individual mechanisms and secure the systems further, two-factor authentication emerged as a strategy that combines two systems. Burnett [13] asserts that security is directly proportional to number of authentication methods used. However, this increase in security brings a trade-off in the form of usability, where the user's burden has increased from one to two mechanisms [65].

Apart from new technologies being evolved, Weirich et al. [92] believed that instead of changing existing technologies, we should change the mindset of people (who are usually referred to as weakest link [72] because they are unable or unwilling to follow security protocols) and persuade them to use secure password practices. Sasse et al. [3] reported that as long as users are aware of the need for secure behaviours, they can be motivated to become security conscious. Whitney identifies that the issue is that users' mental models are inaccurate and incomplete. However, Herley [35] calls users' decisions to avoid security advice entirely rational because the burden to follow the advice is very large compared to the practical gain from the advice.

2.2 Password Problem

A password should be easy for the user to remember as well as hard for others to guess. However, these two requirements often collide and result in the password problem [93], which is well known in research community. Strong passwords are necessarily random and hard to guess, but then they are typically also hard to remember for users. Passwords and their problems have been around for decades. Saltzer et al. [70] highlighted the importance usable security in 1975. Morris et al. [52] discuss password issues in UNIX operating system in 1979. Sasse et al. [3] revealed the lack

of usability in passwords in 1999. Rather than improving, the problem has grown, resulting in an additional burden for users and losses for companies due to leaked or stolen passwords [90].

Passwords have undergone many advancements [26, 40, 43, 52, 94], however, users still struggle with passwords. Florencio et al. [28] analysed the web password habits of 5,544,960 users and found that a user has an average of 25 accounts and 6.5 passwords that are shared across 3.9 different websites, and each user types an average of eight passwords per day. Since users have to deal with so many passwords, they come up with coping strategies [78] like writing passwords down and reusing passwords. Stobert et al. [78] investigated these coping strategies and identified the password life-cycle based on user's password behaviour, detailing the process by which passwords are developed, re-used and adapted.

Despite being claimed dead [42, 82], Bonneau et al. [10] explain why passwords remain; the alternatives are better than passwords in terms of security but are worse in terms of deployability. Herley et al. [36] consider 'passwords are dead' to be an incorrect belief and that it has caused a lot of harm by discouraging research on improving passwords for near to two billion users.

Bonneau et al. [10] introduced a framework for evaluating web authentication schemes in terms of usability, deployability and security. In their associated technical report [9], they provide additional detailed evaluation of password alternatives like encrypted password managers, federated single sign-on, graphical passwords and biometrics.

Bonneau et al. [10] also evaluated encrypted password managers (Firefox [53] and LastPass [44]) as alternative web authentication schemes. They concluded that password managers, as an example of a local single sign-on, have substantial improvements in terms of usability and security compare to passwords. Our focus in this thesis is on password managers [81] and OpenID [64].

2.3 Password Managers

A password manager [81] is a software application that typically stores and organizes passwords in order to replace users' burden of remembering multiple passwords with

just remembering a master password that is used to access all the other passwords. The use of strong site-specific passwords and a reduction in password reuse can be achieved with its help. Also, it is relatively easy to integrate a password manager since it requires no server-side changes in the existing authentication techniques. However, a password manager can be single point of entry and therefore a target for attackers.

Password managers fall in the following categories [29]:

- Client based password managers are typically browser extensions or standalone apps that store passwords in an encrypted database on the client. The stored login credentials are either automatically entered or entered when triggered by the user.

- Mobile password managers store passwords on the mobile device in the form on encrypted database. The user has to view the credentials and type them in, or transmit the credentials through Bluetooth or other secure connection.

- Online password managers store passwords centrally in encrypted form such that a browser extension can fetch, decode and enter them.

- Hashing password managers use password hashing techniques similar to the PwdHash browser extension [68] that derive passwords from a hash of the master password rather than storing passwords, and thus avoid the need to store an encrypted database.

Popular password managers include local password manager like KeePass [38] and cloud based encrypted password manager like LastPass [44]. Often, commercial password managers provide additional features apart from password management. Figure 2.1, reproduced from Klosowsky's recent LifeHacker article [85] offers a good comparison of popular commercial password managers like LastPass [44], Dashlane [21], KeePass [38], 1Password [1], and Roboform [66].

Garfinkel et al. [29] mentions that many password managers have been commercially accessible since the 1990s, but the research on them is scattered. We highlight some of the relevant research projects on password managers.

Chiasson et al. [16] performed usability evaluation of two password managers, PwdHash [68] and Password Multiplier [31], and uncovered significant usability issues.

	LastPass	Dashlane	KeePass	1Password	RoboForm
DESKTOP PLATFORMS	Mac, extensions for Chrome, Firefox, Opera, Safari, Windows Explorer	Windows and Mac, extensions for Chrome, Firefox, Safari, and Internet Explorer	Windows, Mac, and Linux	Windows, Mac, extensions for Chrome, Firefox, Opera, Safari, Windows Explorer	Windows and Mac
MOBILE APPS	Android, iOS, Windows Phone, Blackberry	Android and iOS	Android and iOS via third-party apps	Android and iOS	Android and iOS
PASSWORD STRENGTH REPORT	Yes	Yes	Yes	Yes	Yes
AUTOMATIC PASSWORD CHANGING	Yes	Yes	No	Yes	No
PASSWORD GENERATOR	Yes	Yes	Yes	Yes	Yes
SECURITY ALERTS	Yes	Yes	No	Yes	No
SECURE PASSWORD SHARING	Yes	Yes	Yes	Yes	No
TWO FACTOR AUTHENICATION	Yes	Yes	Yes, with third-party plugin	No	Yes
FORM FILLING	Yes	Yes	Yes	Yes	Yes
SECURITY NOTES	Yes	Yes	Yes, with third-party plugin	Yes	
SYNCING	Yes	Yes, with Dashlane Premium	Yes	Yes	Yes
COST	Free for basic features, $12/year for mobile access, tech support, and extra multi-fac or authentication options	Free for basic features, $39.99/year for secure account backup, unlimited secure sharing, syncing across devices, web access, and priority support.	Free	$49.99 license for Mac and Windows, free on mobile	$9.95 first year/$19.95 after. Standalone Windows and Mac apps available for $29.95

Figure 2.1: A Comparison of Commercial Password Managers [85]

The authors further discussed how these usability issues can pose a major security threat, leaving users more vulnerable than before because they believed that they were protected but were not. Also, participants had inaccurate and incomplete mental models about the working of the software which led them to make errors. The authors also recommended testing security systems for usability.

Stobert et al. [78] designed Versipass, a password manager that does not remember passwords but rather image cues for graphical passwords. These cues help user to recall passwords, associate them with their respective accounts, and re-use passwords in a safer way because Veripass hashes password differently for each account. The authors aimed to combine a password manager and cued graphical passwords for solving password issues like memorability and keeping track of passwords.

McCarney et al. [49] introduced a system called TAPAS as a replacement to traditional password managers. It is a browser extension implemented on dual-possession authentication that involves two applications: a manager (on computer) and a wallet (on smartphone). The Rendezvous server pairs the manager and wallet by scanning a QR code. TAPAS does not require a master password, thus overcoming one major disadvantages of password managers.

Yan et al. [97] designed a cloud based password manager that uses biometric authentication as a second factor to the master password authentication, thereby resolving the single point of entry issue and providing the convenience of anytime access.

Stajano et al. [73] introduced the Pico authentication system based on tokens that store credentials, which do not require a master password to unlock; instead, they are unlocked by the personal aura that digital accessories worn by the user generates. However, it was difficult to embrace since adopting Pico required changes from both ends, user and websites [74]. As a result, the Pico Lens, a browser plugin that makes websites appear as Pico-enabled, was designed, which in a way converts Pico to a password manager. The authors believed that since the users are familiar with the concept of password managers, users would associate password managers with Pico Lens and this would aid in adoption of Pico. Pico Lens locally rewrites the websites' code on the fly, such that they support Pico authentication along with password authentication, so that Pico users would use their Pico to log in.

Usually, websites with JavaScript enabled are difficult to operate by password managers. Stajano et al. [75] suggest using password manager - friendly specifications on websites by augmenting password related pages with semantic annotations. This would help password managers to extract the meaning of the operation to be performed on the web page, thus reducing errors (e.g., saving the incorrect password when authentication fails) and making it more effective.

Password managers are very helpful but sometimes even adults find them difficult to use because different password managers work differently. Also, users feel uncomfortable handling over control of their passwords to a manager [16]. Furthermore, we found no password manager that children could use.

2.4 OpenID

As an alternative to password managers, Single Sign On (SSO) [22, 61] is an access control mechanism that allows users access to multiple resources after initial authentication. It is like issuing the user a single entry token that grants complete access since it is trusted across multiple systems within a single organization. With SSO,

the user has to log in once per session, and the SSO allows access to multiple services without having to re-authenticate during that session. For example, if a user has logged into Gmail, then he is automatically logged into Google Drive, YouTube and other Google services while the session is valid. Single Sign On could be used for user authentication and management across multiple internal services within the organization.

In order to simplify user authentication across multiple organization, applications, and platforms, a new identity management concept known as federated identity evolved. A federated identity results from linking a person's electronic profile stored across various distinct identity management systems [48]. The concept of federated authentication was introduced in 1978 when Needham and Schroeder presented the trusted third-party authentication protocol [54], which along with suggested changes [23], formed the basis of Kerberos [41]. A survey [61] conducted by Pashalidis and Mitchell attests that many proposals for federated authentication on the Web are inspired by Kerberos. Federated identity management can be achieved by open source technologies such as OpenID [64] and OAuth [56].

OpenID [64] is a decentralized user-centric authentication protocol. It allows the same credentials to be used to log in anywhere; however, the user has to log in multiple times unlike SSO where you log in only once per session. For example, you can sign-in Dropbox, Duolingo or Airbnb via your Google account. But, you have to log in every time at each cooperating site using your Google credentials. If you log in to Dropbox, you will not be logged into Airbnb unless you re-enter your credentials at Airbnb.

The most recent protocol to join the OpenID family is the interoperable developer-friendly user authentication protocol known as OpenID Connect [60,69], a layer based on OAuth 2.0 [34]. The OAuth framework is an open standard that provides authentication and authorization as a service. It provides third-party applications limited access to end-users' profiles. OpenID Connect similar to Open ID 2.0 enables developers to authenticate users but without managing or storing passwords.

OpenID does not rely on a central authentication authority, instead, it allows any web server to act as an "identity provider" to any cooperating sites (relying parties),

thus eliminating the need to have separate credentials for each site and reducing password fatigue. Users can create an account with any OpenID identity provider, and use it to log in to any cooperating site. To log in to a relying party [87], the end user enters an identifier which is a URL (e.g., https://username.identityprovider.com), that redirects the user to their identity provider where they enter their OpenID credentials. After successful authentication, the user is redirected to the original relying party site. Tsyrklevich et al. [87] explained the OpenID protocol as illustrated in Figure 2.2. These 7 steps are required to log in the user via OpenID.

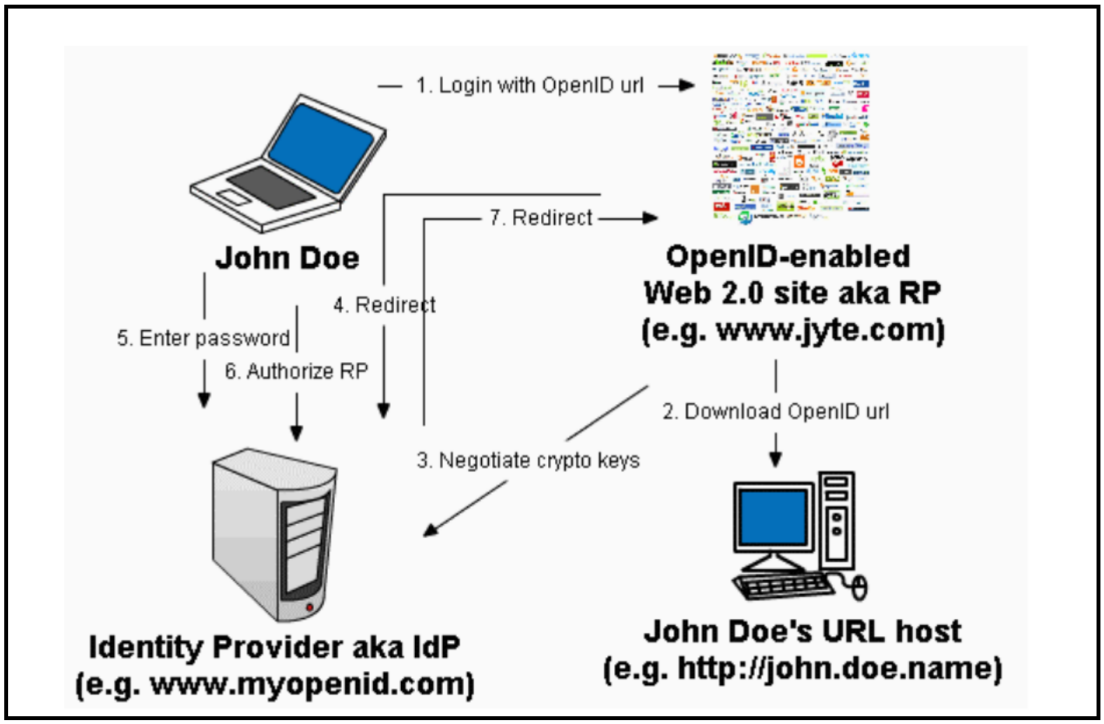


Figure 2.2: OpenID Protocol [87]

Security issues have been identified in OpenID, including flaws [91] that lead to data leaks and redirect users to unsafe sites, phishing attacks [11, 45, 51], covert redirects [83,84] and a lack of privacy [11,88]. For example, phishing [39] is deceiving the user to disclose sensitive information to a genuine looking but malicious website. With OpenID, the attacker can use the genuine website by corrupting it with a malicious login form. Delft et al. [89] provide a security analysis of OpenID and suggest possible solutions. That being said, OpenID is no more or less secure than

the current authentication systems. [59]. However, it does provide benefits [58] like speedy sign up, control over online identity, and minimal passwords.

Even though OpenID addresses usability issues in the password problem, it is facing issues in adoption due the fact that the majority of sites prefer to become identity providers over becoming relying parties [79]. The list [59] of OpenID identity providers include GetOpenId, Google, Yahoo!, WordPress, Verisign, MyOpenId and others.

2.5 Children

Next, we focus on the intended user group for our proposed system. A survey [76] conducted by MediaSmarts in 2014 reported that 99% of Canadian students have access to the internet. This survey included 5,436 students between grades 4 to 11 across the country. Another survey [19] was conducted by Common Sense Media in 2013 reported that 72% of children aged between 0 to 8 years used mobile devices, of which 38% were under the age of two. Both surveys reflect a sharp rise in recent years. Over the years, Canadian parents' sentiments have changed from being enthusiastic to being worried for their child being online [77]. In 2000, parents were enthusiastic about the possibilities offered to children by the internet. However, by 2004, parents no longer saw this increased connectivity as a boon, instead they spent a lot of time monitoring the child's internet usage. By 2011, parents felt insecurity and fear, as they no longer could keep surveillance on their children who used internet across multiple devices. Despite that, a third of Canadian children studying in grade 4-6 are not supervised when they are online. Although children are one of the largest growing users group of the internet, they have received very little attention from the security community. Children are using the internet although it was designed primarily with adults in mind.

Statistics from Australia [2] and UK [80], repeat the same story: 97% of the households with children aged 15 or under provided the children with access to the internet. A recent poll [95] from UK security firm Bullguard reported that 70% of children aged 8 to 12 use the web unsupervised and nearby 34% own a tablet. The

statistics of Australia [2] further reveal that households with children had 7 internet-enabled devices, compared to 6 devices for households without children.

There were various other studies indicating that youth are actively online. A study [46] reports statistics on children's online experience in Europe and what issues they faced. Steeves [76], in "Young Canadians in a Wired World Phase III : Life Online", reports young peoples' perspective, preferences, and behaviour in regards to the internet.

The article "How Young is Too Young? Introducing Young Children to Information Technology" [30] discusses viewpoints on when to expose children to technology. The author suggests that before installing an application, the parents should consider whether the application will provide the child with new learning opportunities. The article further concludes that exposing children to technology for short spans can be advantageous if it does not substitute external activities and involves collaboration.

2.5.1 Online Security and Privacy

Having children online exposes them to risks and raises privacy and security concerns. Halpert [32] suggests educating children about online privacy even before they enter elementary school, because children are surrounded by gadgets from birth and tend to use them without any awareness of how to be safe.

Rode [67] also looks at issues of domestic privacy and security with parents and children under 18. The author advises parents and children on dangers of internet usage as well as provides suggestions for design, ethics, and privacy when working with children. She found that children do not understand the technical language used in security warnings and so cannot take proper action to protect themselves. Further exploring children's understanding of security and their language surrounding it, the study [62] "Under my pillow: designing security for children's special things" was carried out with children of aged 8-10 in order to design the security features of a mobile application for children. The authors concluded that children's notion of security was limited. Children understood conceptually but their actions revealed a gap in their ability to apply the concepts to real life situations. They discuss how children mention not sharing secrets with strangers but they did not consider the

just-met researcher as a stranger. Also, one child participant could not spell her password and called across the crowded room to ask, unaware that she was revealing her password to everyone.

2.5.2 Parental Control

Research in online security of children has majorly focused on parental controls or similar monitoring tools. We summarize a few relevant research projects.

Channakeshava et al. [14] describe an automated tool named POCKET (Parental Online Consent for Kids' Electronic Transaction) to enforce COPPA (the US's Children's Online Privacy Protection Act). According to COPPA [18], the collection of information from children under 13 needs parental consent. POCKET helps parents enforce policies limiting access to online resources and protect their child's privacy.

Fahrnberger et al. [27] propose a framework called SafeChat, which filters incoming abusive words from child devices and provides security by providing message encryption as well as parental monitoring. It is intended to aid in reducing cyberbullying."SafeChat is an amalgamation of the 4-layer Context Based Authentication Framework (4-CBAF) and the cryptosystem SecureString 2.0 [27]".

A US patent was filed for a system [17] to provide restricted, but secure, internet access to children under parental control settings. The system includes a Safe Card with integrated biometric fingerprint scanner and USB card reader. Parents register their child, scan the child's fingerprint, and set parental rules. The child can insert the card reader into any device's USB port, then insert their smart card, allowing the child restricted access the internet as permitted by the parental rules. The child cannot access the internet on computers with SafeCard installed without the device.

In 2008, a Near Field Communication enabled school attendance system was tested. The study [25] for monitoring attendance was carried out with children between 6-8 years old in a primary school. Students had to tap their card on a card reader to mark entry and exit from school. Results showed that all users (teachers, parents and children) benefited from this digital attendance system. The attendance process became fast, accurate, and convenient. The system created logs for teachers and enabled parents to check their child's attendance in real time.

Barron [6] describes how children between 8-12 years respond to surveillance. "Children are not passive recipients of parental surveillance and power, rather they are increasingly playing an active role in negotiation with parents and actively resist monitoring of their everyday lives." She also explains that children prefer less disruptive communication such as text messages over calls from their parents. The study also explores how children circumvent surveillance, for example, by texting to their parents that they are at a permitted location when they are actually somewhere not allowed without permission.

2.5.3 Authentication

Children, like adults, suffer from issues related to the password problem but only a few studies have looked at authentication for children. We summarize their results below.

Read and Cassidy [63] carried out two user studies with children of age 6-10. The first study revolved around children's knowledge of how to create good textual passwords, while the second investigated passwords children used. An interesting finding was that children saw passwords as keys to stop people from entering rather than something to let the user in. The younger children used comparatively shorter passwords, but everyone made simple passwords. Read and Cassidy suggested three textual password design principles for children. The principles related to length, composition, and warnings.

Mendori et al. carried out a study [50] to design a new password input interface for primary school children who are not familiar with the Roman alphabet. The new mouse-based password input interface used icons already familiar to primary school children, like fruits, insects, animals, flowers, colors and symbols. The interface shuffled the location of icons with each login, so the password cannot be guessed if only location of selected icon is known. Variations in the number of icons were evaluated. The configuration with 16 icons and 3 selections was found the quickest, but the children made mistakes in input order.

Tse et al. propose a multi-level authentication scheme [86] similar to a game for young children. Instead of memorizing a textual password, the children answer

challenges. The challenge responses are stored and compared the next time the same challenge is played. Multiple verifications occur between the device and the user causing the process to be a little longer and require training. No implementation of the proposed work was found.

Recently, a password authentication [37] comparison was carried out between children and adults using three graphical password schemes (Object, Image and Word Pass Tiles) where they must select their previously memorized image from tiles among a grid of decoys. The systems differed in the types of images contained on the tiles. Children preferred and performed better using the Object Tile scheme that displayed one easily distinguishable object per tile. General recommendations included "Adapt interface to be age-appropriate", highlighting that children have different authentication needs than adults.

Summarizing the studies, we can say that text passwords are difficult for children to remember and spell accurately. Graphical passwords and/or icon passwords appear more viable for children.

2.5.4 Designing and Methodology

Bruckman et al.'s "HCI for kids" book [12] explains how to design for children. It not only describes how children differ from adults but also how children from different ages change in abilities. They caution that designers often design based on their assumption of childhood. The authors recommend age appropriate interfaces and suggest that touch interfaces are better than mouse input. Our target child age group is 7-11 years, which Bruckman et al. [12] call Concrete Operational and describe as: "Concrete Operational children are old enough to use sophisticated software but still young enough to appreciate a playful approach". Druin et al. [24] investigated how children aged 7 to 11 searched for information online. They found distinct difference between the younger and older children. For our study, we wanted children who could read and spell but who were still young enough that they would require parental consent or assistance to log in. Furthermore this age range allowed us to identify any distinct behaviours among and younger and older children.

The summary "Kids and the Internet" [7] explains that preschool children (2-5

years) need more verbal instructions as they have less tolerance technical difficulties and shorter attention spans. As a result, their tasks should be easy one click tasks that provide immediate feedback. Young school students (6-9 years) can read instructions. They can operate well on composition-based and strategy-based activities. Tweens (10-14 years) are capable of performing more difficult tasks. Different age groups have different needs and those needs are different from those of adults.

The design principles [7, 12, 62] we found relevant to our work are: to involve children in the design process, use metaphors when explaining tasks, target a specific age group, keep the error messages simple, and keep the application interactive.

2.6 Summary

There are recent advancements in the field of authentication and password managers, but the password problem still exists. The usability issues are even more pronounced for children. Children represent a significant online user group yet child authentication has received little attention by research or commercial communities. We are working towards an authentication alternative for children in the form of a password manager that is managed by the parents. This thesis covers the iterative design process, prototype development, and evaluation of our proposed system.

Chapter 3

Low Fidelity Prototype Design and Evaluation

There is sparse research on child authentication and the majority of solutions are parental controls. We suggest a parent-child password manager as a viable solution. To our knowledge, no child specific password manager exists. In this chapter, we describe our proposed parent-child password manager along with its user study.

3.1 Prototype Design

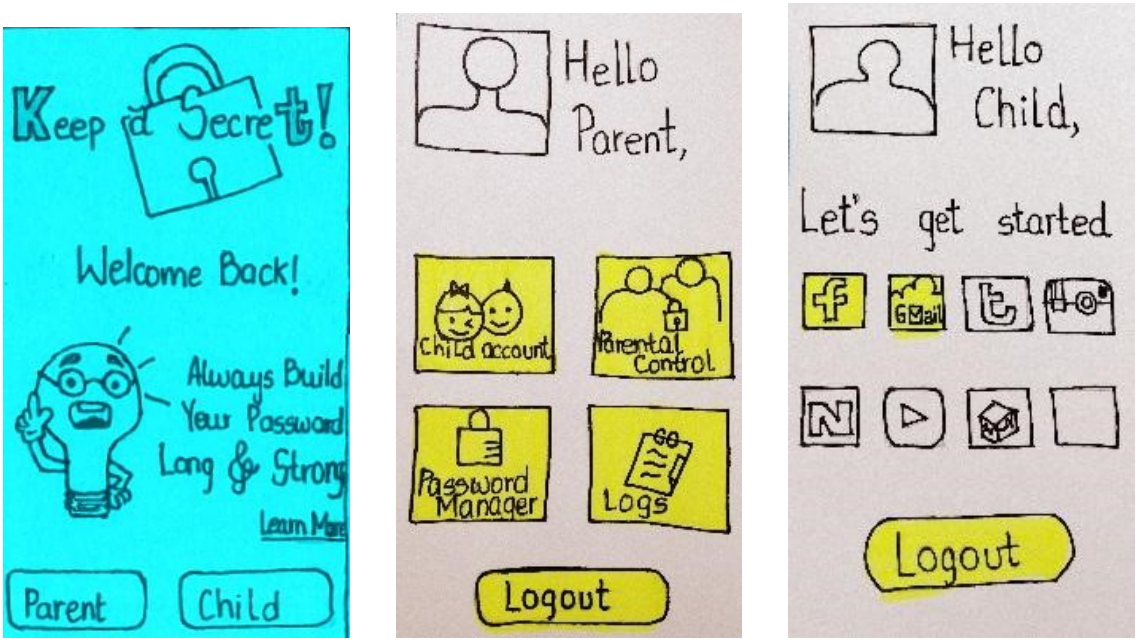
After initial brainstorming, we created a low-fidelity prototype which allowed users to interact with our design and enable us to gain feedback in order to refine the design. A low fidelity prototype [4] helps to explore design alternatives quickly and at a low cost. Furthermore, it is relatively easy to detect and fix problems early and at minimal cost with these prototypes.

We sketched a low fidelity prototype on paper which was made interactive by using Prott[1]. It is a rapid prototyping tool that lets you sketch your idea on paper, then links the initial sketches by adding transitions and gestures, thus making the sketches interact like a real app. We initially designed the proposed password manager as a mobile app because of the popularity of mobile devices within this user group. The prototype consisted of 25 individually sketched screens.

Our proposed 'Keep A Secret' is a parent-child password manager for children aged between 7–11 years. It remembers passwords for children and assists the parents in keeping children safe by providing login history. Also, parents can control which sites the child can visit and when. This prototype removes the burden of remembering multiple passwords from children and replaces it with master password and parental permission.

The prototype is devised with two user categories in mind, child and parent, as

[1] `https://prottapp.com/`



(a) First page of the Password Manager prototype.

(b) Home page when logged in as parent.

(c) Home page when logged in as child.

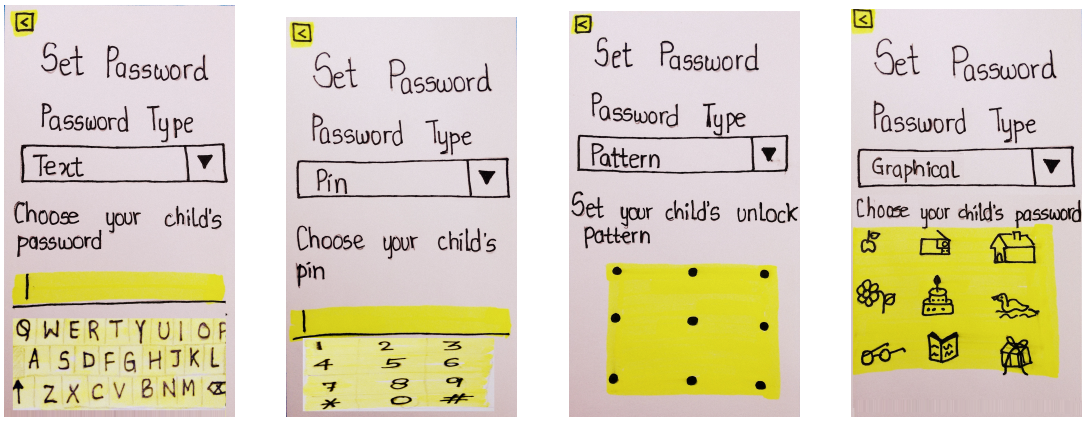
Figure 3.1: Low fidelity Prototype

shown in Figure 3.1a. Once set up, children uses the app as the gatekeeper for all of their online accounts. A child enters their master password and taps the site they want to visit (Figure 3.1c). The password manager enters the stored account credentials and allows access to the account, provided that the predefined parental rules permit access. The parent would register themselves, and then can set up a child password manager account, add child online accounts and their passwords, enable specific permissions for online accounts and view logs (Figure 3.1b).

3.1.1 View as Parent

When the parent logs in with an alphanumeric password, the homepage provides parents with the following four options as shown in Figure 3.1b.

Child Accounts: Parents can create password manager accounts for each of their children and set up the children's master password. In the prototype, we presented an option to select a password type (text, PIN, pattern and graphical passwords) for the child's master password as shown in Figure 3.2.



(a) Alphanumeric (b) PIN (c) Pattern (d) Graphical

Figure 3.2: Master password Types

The four options were as follows; specific password rules were not defined at this early stage. An alphanumeric password (Figure 3.2a) is a combination of letters and digits. A PIN (Figure 3.2b) is a combination of only digits. A pattern (Figure 3.2c) consists of connecting dots with one continuous gesture. A graphical password (Figure 3.2d) involves selecting a sequence of images from a panel of 9 icons.

Password Manager: After setting up a child's password manager account, the parent adds online accounts like email or games that the child can access. The parent can save pre-existing credentials or generate a strong password automatically for new online accounts. Currently, the password manager is intended for login with the credentials through websites only.

Parental Controls: Parents can set controls for their child's online activities. The *Scheduling* option allows parents to specify times when a particular online account can be accessed. The *Website Permissions* option enables or disables access to a particular online account entirely.

Logs: The history of the child's online activities as captured through interaction with the password manager is provided in logs. The parent can view the login times and websites that a child has visited.

3.1.2 View As Child

When a child opens the app, a password entry screen for one of the four types (alphanumeric, PIN, pattern and graphical) is shown as in Figure 3.2. The child logs in with their master password that was set up from the parent account, and they can then access all the accounts that their parent permits without requiring individual passwords, as shown in Figure 3.1c. If they forget the master password, an email requesting to reset it is sent to their parents.

3.2 User Study

We conducted a user study to evaluate the usability of our low-fidelity prototype and get feedback from parents and children about what they would need from a password manager. The goal is to gauge the appropriateness of the prototype and identify areas of improvement. We also collected information about current website, login and monitoring activities.

This research was approved by Carleton's Research Ethics Board-B. The interviews took place at a public location of the parent's choice. Each parent-child pair completed an in-person individual session with the experimenter which lasted about 60 minutes. A session had two parts, one with the child and one with the parent. The children were tested first, and then offered some activities (e.g., colouring or small crafts) while the parents completed their part. Each part followed the same general process:

- A pre-test interview: We asked participants about their current knowledge and use of passwords, and some basic demographic questions.
- Prototype testing: Participants interacted with the prototype and gave us feedback. They were encouraged to comment while interacting with the prototype.
- Post-test interview: We conducted a brief interview pertaining to their experience with the prototype.

We audio-recorded participants' verbal feedback (with their consent) and transcribed the audio files. We also took written notes during their interaction with the prototype.

The participants were shown the low fidelity prototype on a smart phone, where images were sketched on paper and navigational links plus animations were added to it via Prott to make it minimally interactive. Tasks were assigned to see if the user understood the flow of the prototype. The user could not input anything, but could click and navigate to linked pages. They were informed that everything click-able was highlighted in yellow.

3.3 Study Protocol

The study protocol consisted of the following steps:

1. Greeting: Participants were greeted. The experimenter explained the purpose of the study and also made clear that it was to test the usability of the password manager and not them (as for many this was the first user study).

2. Consent process: The parents were asked to read and sign the consent form for adults and child participation if they were comfortable with having their child participate in the study. Verbal informed assent was obtained from the child if they agreed to participate. It was emphasized to the participants that their participation was entirely voluntary and that they may stop at any time. Parents were nearby and were allowed to monitor their child's session if they wanted.

3. Session with Children

    (a) Children answered pre-test interview questions (Appendix A) and we audio recorded their responses.

    (b) Children interacted with the prototype to complete the following tasks:

        i. Click Child – Select the user category by tapping the "child" button on the welcome screen.

        ii. Login – Sign-in by entering a username and password, assuming that the credentials had previously been set up from their parent's account prior to signing in.

iii. Navigate to websites – Navigate to any two websites by clicking any two online account icons on the homepage.

iv. Logout – Logout by clicking the "Logout" button on the homepage.

(c) After the tasks, we showed them the four password types (text password, PIN, pattern and graphical password) as shown in Figure 3.2, and explained their functionality using a paper prototype. Children chose which they wanted as a master password and indicated which they disliked. They provided reasons for their selections.

(d) Children answered post-test interview questions (Appendix A) and their feedback was recorded.

4. Session with Parents

(a) Parents answered pre-test interview questions (Appendix B) and their responses were recorded.

(b) Parents interacted with the prototype to complete the following tasks:

i. Click Parent – Select the user category by tapping the "parent" button on the welcome screen.

ii. Register – Register as a new user by entering their name, username, email and password.

iii. Login – Sign in by entering the username and password.

iv. Create Child Accounts – Create an account for a child and set a master password for the child by navigating to the "Child Account" screen. To set the master password, parents had to select a password type. They were shown on paper and verbally explained the four password types and then were asked which they preferred and which they disliked for their child. They provided reasons for their selections.

v. Access Password Manager – Add an online account for the child by navigating to the "Password Manager" screen. While adding a website, the parents were asked if they prefer to manually create a password or have the system generate a password.

vi. Access Parental Controls - Scheduling – Add a schedule specifying when the child can access their online accounts by navigating to the "Parental Controls" screen.

vii. Access Parental Controls - Website Permissions – Disable a child's access to an online account by navigating through "Parental Controls".

viii. View Logs – View which online accounts a child visited today by clicking "Logs" on homepage.

ix. Logout – Logout by clicking the "Logout" button on the homepage.

(c) Parents answered post-test interview questions (Appendix B) and their feedback was recorded.

5. Wrap up: We thanked the participants for their time, answered any questions, and provided them with the honorarium.

3.3.1 Participant Demographics

In all, ten parent-child pairs participated in the study (20 participants). They were recruited for this study via invitations through our network of acquaintances and local parenting groups on social media. Only those children who were regular online users and aged between 7-11 years were allowed to participate, along with their parents or guardians. Among children participants, we had 6 girls and 4 boys (mean age of 9.2 years old). We had children from grades 1 to 6 (mean grade 3.8). Two of ten children were home-schooled. For the parent participants, we had 7 mothers and 3 fathers. Table 3.1 details the participant demographics.

3.3.2 Data Collection

Data was collected through the following methods.

- Audio recorded pre / post interviews answers.
- Written notes of observation of the participants interacting with the prototype as they complete the tasks.

P#	Child Age	Child Grade	Number of Child Accounts	Child Gender	Parent Gender
1	7	1	4	f	f
2	7	2	5	f	f
3	8	3	3	f	f
4	9	3	4	f	f
5	9	4	3	m	f
6	10	5	3	f	m
7	10	5	3	m	f
8	10	4	6	f	m
9	11	5	5	m	f
10	11	6	7	m	m

Table 3.1: Participant Demographics

- Written notes of the verbal comments made by participants while interacting with the prototype.

The audio recordings were transcribed by the experimenter. This qualitative data was analyzed with the aid of Atlas.ti[2]. Atlas.ti provided tools to evaluate and visualize relationships in the data. It helps to collect all the research data in one place, code it, and analyze it.

We analysed the data on a per question basis, tabulating the data based on common ideas and noting any interesting outliers. The interview transcripts were tabulated using descriptive codes by the experimenter. Since the questions were very straightforward, we did not use another experimenter for second analysis.

We classified the data in five general categories:

1. Demographics: We recorded gender, age, grade, and number of online accounts and passwords.

2. Password knowledge and habits: We derived this data from interview questions covering the definition of "passwords", password sharing habits, and creating and forgetting password scenarios.

[2] `http://atlasti.com/`

3. Password type preferences: Participants indicated their most and least preferred choices from the 4 password types, along with their reasoning.

4. Tasks accomplished: We recorded if the participants completed the tasks without help, completed them with some help, or did not complete them.

5. Prototype feedback and suggestions: Participants provided their feedback on the prototype and suggested improvements.

3.4 Results

Based on our data classifications, following are the results from each category:

3.4.1 Demographics

We found no apparent relationship between gender, age and number of accounts or passwords for the children. However, older children generally knew more conceptual details regarding passwords and online safety.

As seen in the Figure 3.3, tablets are the most popular devices used by children, followed by desktops and phones. The majority of parents reported their children using multiple devices. Thus, they wanted an authentication solution for their children that can be accessed from multiple devices.

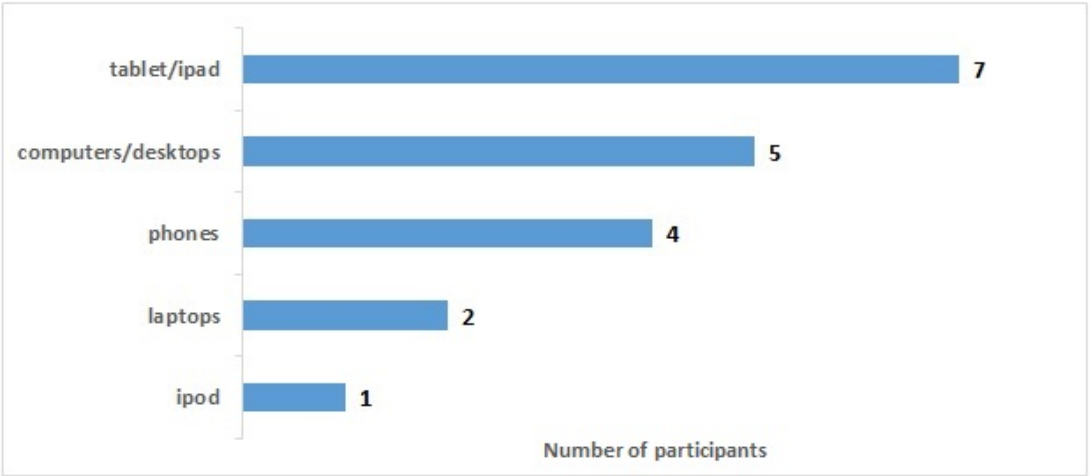


Figure 3.3: Device Usage for Children. Multiple responses were allowed.

3.4.2 Password Knowledge and Habits

Children had passwords for between three to seven accounts. We asked both the children and parents questions about who creates the child's passwords and how many accounts the child has. Interestingly, parents' answers did not always match with their child's response. When asked who creates passwords for child accounts, four parent-child pairs had a mismatch in responses. For example, one child said that he creates his own passwords while his mother said his elder sibling creates them. Similarly, on inquiring about the number of accounts or passwords, seven parent-child pairs had different numbers. It is unclear from our data whether these mismatches are because parents are unaware of their child's activities, whether they interpreted the questions differently, or whether they simply misremembered.

On asking the participants what issues they faced with children's passwords, nine parents responded with forgotten password and/or devices being locked due to multiple incorrect password attempts. One parent reported that his child claims his account has been hacked and thus changes password frequently.

We also inquired about coping strategies. Six parents admitted that they re-use passwords for their child's accounts. However, only three children mentioned re-using passwords. One child and four parents admitted to writing down passwords on places like sticky notes pasted on computers, calendars, Excel spreadsheets and emails. To simplify access, the majority of family devices had no password.

The children's answers to the question "What is a Password?" are displayed in Table 3.2. Most children viewed passwords as a barrier to keep unauthorised people from gaining access, although several had difficulty articulating exactly what they meant. A few mentioned the concept of protecting personal or private data, or keeping something safe or hidden. The majority of children liked the idea of using one master password to access all accounts; only one child completely disliked the idea because he thought this was insecure. Three children suggested modifications as they felt using one password was not enough to protect all their accounts.

Very few parents used parental controls in any form. Among those who did, they mentioned age restrictions, Netflix child accounts, Rogers parental controls, or other filters. No one used a password manager for their child.

Participant	"What is password?"
Child-1	"A password is something to block your electronics. A password is something to protect your electronics from getting like privacy out by hackers and a lot of other villains that try to hack computers."
Child-2	"We use a password so that we can keep our information safe."
Child-3	"So people can't get on the phone."
Child-4	"For somebody, takes her (mom's) phone, and can't know the password."
Child-5	"It is something to keep something hidden from someone."
Child-6	"It's password is.. it means that.. so you , let's say you have a password on your may be, let's say a game, you have to have a password because, it means that, because if you know it, you can get on, but the only way that other people, because they may know what your username is, so if there weren't any passwords then you wouldn't, then they could just go onto your account."
Child-7	"It's basically something, kinda to, it's kind of like a code that you have to know to get into something."
Child-8	"It is something so that people can't get into your accounts and information."
Child-9	"Password is something that keeps all your personal stuff safe."
Child-10	It's like a quarter of a word, like to get into a computer or phone, that someone else can't really guess."

Table 3.2: Children's definition of "Password"

Children have various self-defined heuristics about sharing passwords. All children agreed to sharing passwords with parents and denied sharing passwords with strangers. Questions arise about who children consider a stranger. In our study, the interviewer was apparently not considered a stranger for two children who were about to share their exact password when asked to define password. This is similar to findings from Read and Beale [62]. When questioned about sharing with friends and teachers, the majority said they would type in passwords for friends, rather than sharing, and agreed to sharing only school accounts with teachers since the teacher already has those details. Figure 3.4 summarizes these password sharing results.

We provide quotes illustrating a few participants' responses to various scenarios in Table 3.3.

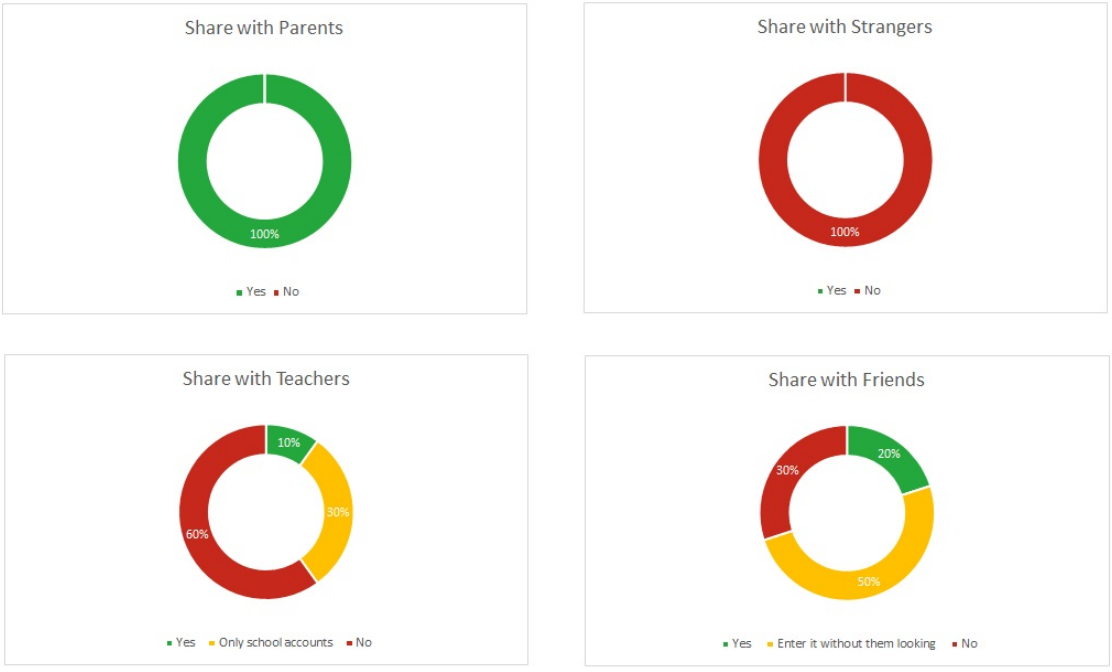


Figure 3.4: Password sharing tendency in children

Child	"passwords should be easy to remember like birthdates."
Child	"My mom says not to share passwords. But if they need it then give."
Child	"I have memorized my school password since it's the same since 2 years"
Parent	"I use the same password repeatedly so it sticks with him"
Parent	"we keep passwords that she remembers like her name or horoscope number."
Parent	"We write the password for computer, we write the username and password and this will make it easy for them. Yeah, there's a sticker on the computer."
Parent	"We have had the talk but I know they share passwords at school"

Table 3.3: Quotes from participants regarding password habits.

3.4.3 Password Type Preferences

The majority of children preferred graphical passwords, while the majority of parents preferred PINs for their child's accounts. Parents most disliked pattern passwords. Children disliked text and pattern passwords. Figure 3.5 summarizes the child and parent preferences. Two parents later changed their preferences when they became

aware of their child's preference, either by asking their child directly or when overhearing their child's response.

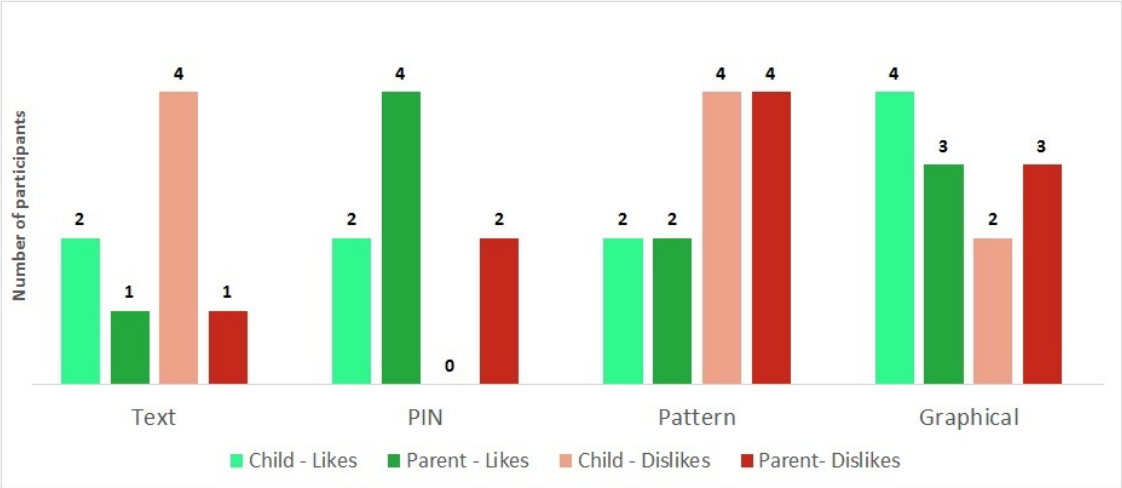


Figure 3.5: Password type Preferences

3.4.4 Tasks Accomplished

Parents and children were given interactive tasks such that they had to click the yellow highlighted areas on the screen and navigate accordingly to complete the specified task. The results of the tasks can be: completed successfully, completed with help (the experimenter hinted that either the task is incomplete or incorrectly completed), or incomplete.

The majority of children successfully completed all tasks. A few were unfamiliar with a login screen (Task-Login). Further inquiry showed that parents for these two children enter the passwords for their children. Two children attempted to log in as a parent instead of child because they were curious (Task-Click Child). A few children were unsure which two accounts to proceed with when given a choice to log in to any two accounts via the prototype (Task- Navigate to websites). However, everyone could logout (Task-Logout). Completion results for children are summarized in Figure 3.6.

All parents clicked the parent button for 'Click Parent' task. On seeing the login screen, six registered as new user while four were unsure whether the experimenter

would provide credentials (Task-Login). The majority of parents got confused between tasks involving parental controls and the password manager features. Everyone initially clicked on the parental control icon, while executing the password manager task. Parents were subsequently aided in executing the parental control tasks because they had already previewed them (Tasks - Access Parental Controls - Scheduling , Access Parental Controls - Website Permissions). A few parents required hints in the 'view logs' task because they were searching for the term 'history'. Only two parents wanted to use the generate password functionality willingly; another four explored the functionality but chose not to use it. Finally, a few users got confused between back and logout icons available at the top corners of every screen. For example, four users clicked the logout icon when asked to use back icon to return to the homepage. Results for the parents' tasks are summarized in Figure 3.7.

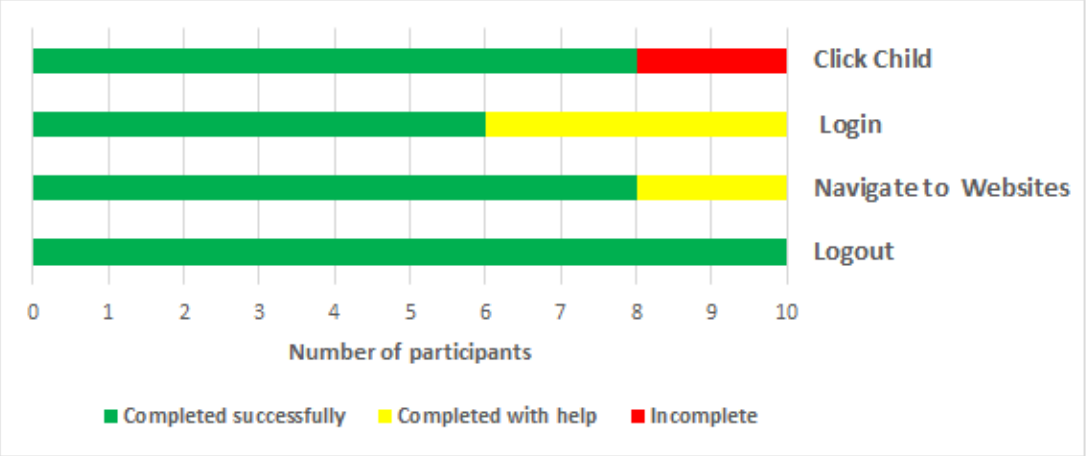


Figure 3.6: Completion status of Child Tasks

3.4.5 Prototype Feedback and Suggestions

Seven parents said that they liked the prototype and would use if it was available. The others said they liked the prototype but that they would not use it because of previous bad experiences with password managers or because they felt it was unnecessary since they trusted their child.

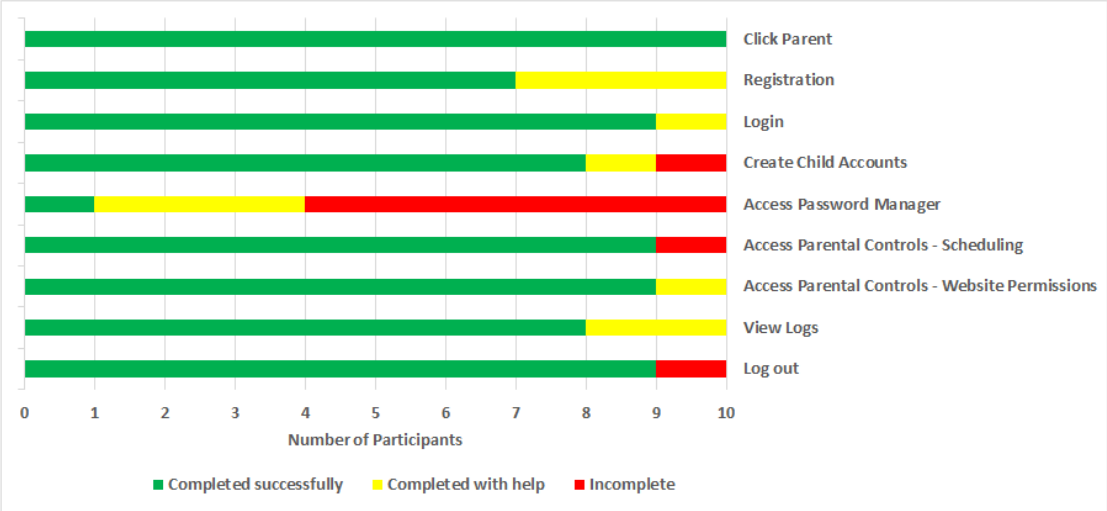


Figure 3.7: Completion status of Parent Tasks

We further asked participants to suggest modifications. These suggestions were analysed and categorized as shown in the affinity diagram from Figure 3.8. We grouped suggestions from children and parents together.

Password Suggestions: We provided four password types (text, PIN, pattern and graphical) to the participants. A few children suggested using two-step authentication so that if someone gets their password, then they do not get access to all their games and accounts. Some parents suggested adding the ability to draw a password, which is interesting given their dislike of pattern passwords, or using fingerprint login. Participants considered 4-digit PINs and 4-image graphical passwords as weak for the child's master password, perhaps not understanding that the actual website password was stronger. They suggested increasing the grid size and/or the number of selections.

Naming Features: The majority of parents got confused in password manager and parental control tasks because of the icon names. Thus, participants suggested renaming some features. They wanted the "Password Manager" to be renamed to "Website Passwords", "Add Websites" or "Manage Sites". They also suggested renaming "Parental Control" to "Schedule Manager" or "Website Controls" and they

wanted to rename“Logs” to “History”.

User Interface: Some parents suggested to making the interface more visually pleasing and personalising the pages. Others asked to reduce the number of clicks and make navigation more evident by providing descriptions or hints. A few requested making the system seem more legitimate by having the interface confirm all the details.

Functionality: Most participants liked the functionalities provided. Some requested total surveillance; for example, a parent wanted to be able to read her child's text messages. While others said they would prefer fewer controls and said that they would not set permissions. Parents wanted the app to be free and device independent. Other suggestions included adding email/phone notifications, a view-as-child option, a password strength meter, and age restrictions.

3.5 Discussion

This section discusses our findings of this user study.

Mismatch between user mental model and system model: Users develop functional understanding of a system when they interact with it. This is called the user's mental model. It may or may not be technically accurate, and keeps on evolving based on their interactions [55]. The system model [55] is the model describing the actual system and its interaction with users. In ideal world, user mental models and system models match. In our study, there were mismatches between users' mental models and the system model. For instance, some parents explained the major functionalities of the prototype from the homepage, but struggled to navigate through the system to complete tasks because things were not where they were expected. Another mismatch was apparent when participants preferred PIN, graphical, or pattern passwords over each other because one was more secure, when they all have very similar password spaces. Password space refers to the set of all possible password combinations for a given configuration. Larger password spaces are generally more

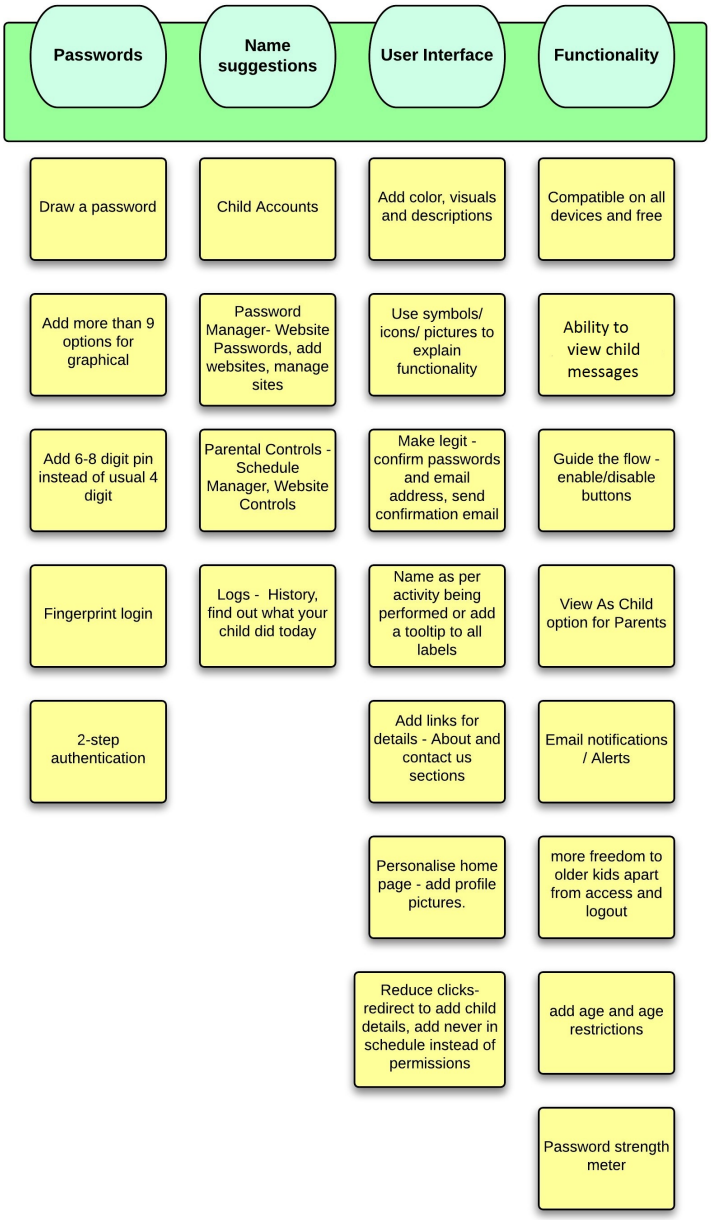


Figure 3.8: Suggestions

secure.

Parents found calling the system a "Password Manager" misleading because when they heard the name, they were expecting to see a traditional password manager application with names of websites and their passwords, but that was not the case when they logged in. For the same reason, a few found the names of the features ("Password Manager", "Parental Controls") misleading too. The most preferred feature of the prototype was the "Parental Controls", which allowed parents to set website permissions and schedules. They suggested using a name that would encompass all the features of the prototype. Furthermore, several added that they were less interested in the password manager functionality and more interested in the website permissions and schedule options of this prototype.

Relationship between parent and child proficiency: Although we did not collect detailed demographics of parents, our data reflected a relationship between parent and child proficiency with respect to the interview questions asked. When parents knew about online safety and talked about it with their children and when they involved children in setting up accounts, these children had higher understanding of passwords and their importance compared to children who were just constantly monitored or for whom parents typed in the passwords. We did have a few parents admit that they did not take any steps towards the online safety of their children and that they never really talked about such topics. Our analysis showed that those children were more likely to share passwords, even with strangers (i.e., the experimenter).

Mismatch between parent and child response: Initially, children were asked how many accounts/passwords they have, who creates them, and with whom they share these passwords. Similar questions about the child were asked to the parents. Even though all the pairs admitted to sharing passwords, only two pairs had matching responses when asked about the number of accounts/passwords. More interesting, were instances where the parent and child had contrasting replies to "Who creates the password?", suggesting that parents may not know about all of their child's accounts or that parents and children have different interpretations of the question.

Barriers to adoption - fears of using a new technology/features: All the parents said they liked the password manager prototype. But later when asked if they would use it for their children, three parents said no. Also, four parents would not use the "generate password" option even after admitting it to be useful. When observing parents perform tasks, the researcher found them hesitant when using any new feature. Some parents just glanced at the new feature, while others explored them briefly but said they preferred their usual way because it is more familiar to them.

3.6 Summary

Based on the results of this study, we conclude that most parents are willing to use an application that would help them monitor their children and keep them safe. Their preferences suggest a password manager with parental controls. As a parent said, "I was not looking for something like this, but now that I see it, I definitely would use it for my kids. Especially the permissions section." Keeping in mind the requirements of the parents and the aim of removing the password burden from children, we discuss our improved password manager in the following chapter.

Chapter 4

KinderSurf - Improved Prototype Design

In this chapter we describe our improved parent-child password manager, named 'KinderSurf'.

4.1 Overview of Prototype Design

Based on feedback from previous study, we redefined the password manager prototype. We created a medium-to-high fidelity prototype which allowed users understand the working of the prototype and enable us to determine its usability. A high fidelity prototype [4] helps to refine requirements and design details and thus guide implementations.

This research is a joint project between our Carleton research team and Bluink Ltd. [1], a local Ottawa technology company. At this stage of the project, we were introduced to Bluink through a mutual acquaintance. Initial conversations revealed similar interests and complementary skills. We, therefore, decided to collaborate with Bluink on the next iteration of the prototype. Bluink has infrastructure in place through their password manager products and can implement the server-side and communication protocols. We defined the user interaction model and workflow, designed the UI, and conducted user testing. This second prototype reflects the insight gained from our first prototype and study, as well as input from Bluink with respect to a feasible system based on their technology.

We developed a digital mobile app prototype using Appery [2]. It is a rapid development platform that lets you create and run apps. We designed the proposed password manager as an iOS mobile app that consisted of 17 individually interactive screens and a few pop-up on these screens. Bluink developed the back-end and push

[1] http://www.bluink.ca/
[2] https://appery.io/

notifications feature of the app for parents to interact and understand the underlying idea of this app.

Our improved 'KinderSurf' app is a parent-child password manager for children aged between 7–11 years, that would enable parents to provide consent without being in close proximity, in order to authenticate the children, when they log in to supported websites. Our proposed authentication mechanism will be achieved using OpenID Connect technology. Furthermore, push notifications and Bluink's Relay service initiate and establish connection between a parent's authenticating device and child's accessed website. Thus, we reduce the burden of multiple passwords to just one pair of credentials, accompanied with parent permission as second step in authentication process.

The prototype is devised with two user categories in mind, child and parent. After a parent has registered with the KinderSurf, they would receive a push notification on every login attempt of their children, as shown in Figure 4.2. The parent/s would receive this notification on all registered devices. The notification would disappear after it is approved or denied by any one of the devices. These notifications can be set to automatically approve or deny via the Rules feature discussed later (Section 4.3.4). Figure 4.3 illustrates how a child would request to log in to the 'Gator Games' website and be authenticated based on the parent's consent. A general overview of the interaction is provided in Figure 4.1.

At this stage, KinderSurf consists of two complementary prototypes, each demonstrating different features. Ideally, we would have one prototype that incorporates all of the desired functionality based on our design. However, this was not feasible given our industry collaborator's time constraints and development cycle. Therefore, this resulted in two complementary prototypes that together cover the full range of functionalities. We describe both prototypes next. Details of the communication protocol are described in Section 4.4.

4.2 KinderSurf - Basic Communication Prototype

We worked closely with Bluink on defining how 'KinderSurf' would work. While we designed the front-end, Bluink worked on the back-end. Time constraints meant

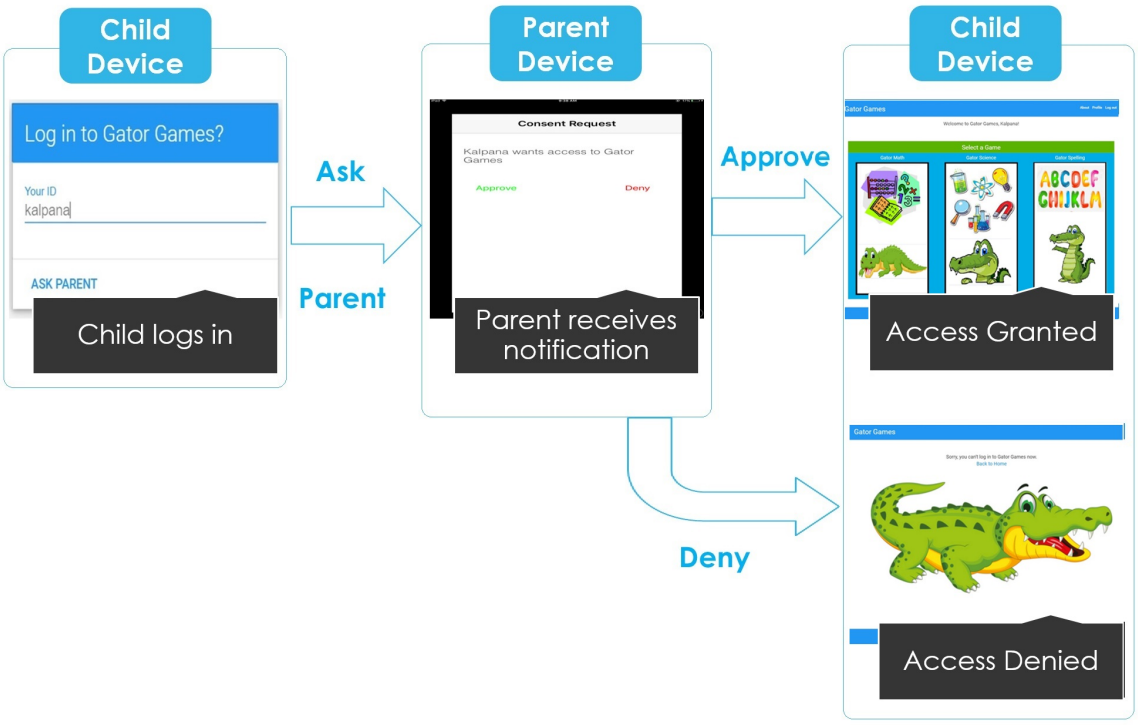


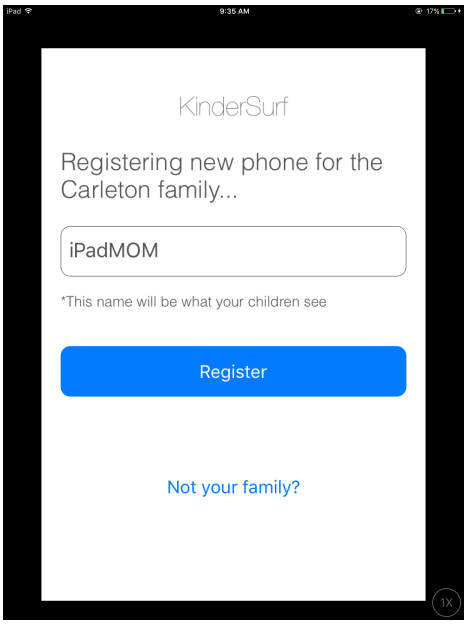
Figure 4.1: Interaction Overview

that a fully integrated and functional prototype was not possible. We instead tested the prototype from Bluink with basic communication regarding authentication. The parents tested the prototype on an iPad while the children used a laptop to access it. The parents were aided to form a mental model with this prototype.

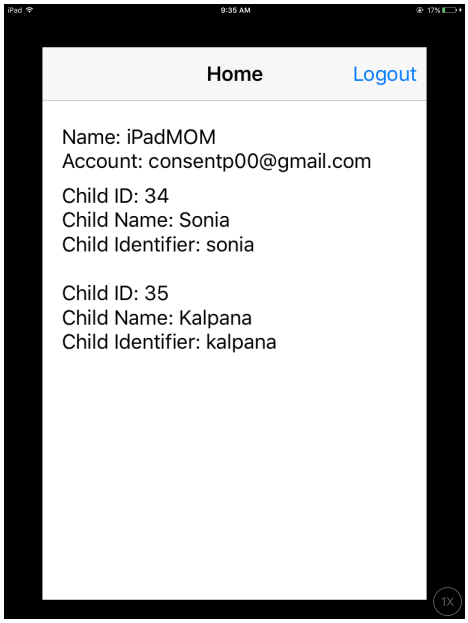
4.2.1 Parent Interaction

For demonstration purposes, Bluink developed an iOS app with basic authentication functionality for parents and provided mock accounts for testing. First a parent logs in with the provided credentials (Figure 4.2a), and then registers their device to receive notifications (Figure 4.2b). After the parent logs in, the Homepage displays the child account details (Figure 4.2c). Parents created a 'Child Identifier', which would be used as a username by the child to request access to any supported website. On each child request, the parents receive a notification displaying the child name and the target website. Parents can approve or deny the authentication request (Figure 4.2d).

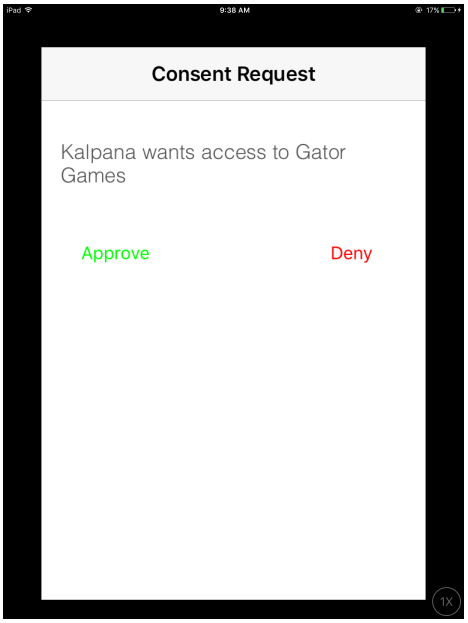
(a) Login



(b) Register Phone



(c) Child Accounts



(d) Parent receives Push Notification

Figure 4.2: Basic Communication Prototype - Registration and Notifications

4.2.2 Child Interaction

For demonstration purposes, Bluink developed a website named 'Gator Games' that supported OpenID Connect technology, and provided an option to 'login with KinderSurf' (Figure 4.3a). When children click on login, they are asked to provide an ID,

i.e., a child identifier created by their parents (Figure 4.3b). This ID links the parent's and child's accounts, and is used to identify the child and send notification to their parent. To log in to a website, the child clicks 'ask parent', and a notification (Figure 4.2d) is sent to their parents requesting access. The child is notified to wait while their parent grants (or denies) permission (Figure 4.3c). If the parent approves the request, the child is logged into the website as shown in Figure 4.3d. Conversely, if the parent denies access, the child is not allowed access to website, as displayed in Figure 4.3e.

4.3 KinderSurf - User Interface Prototype

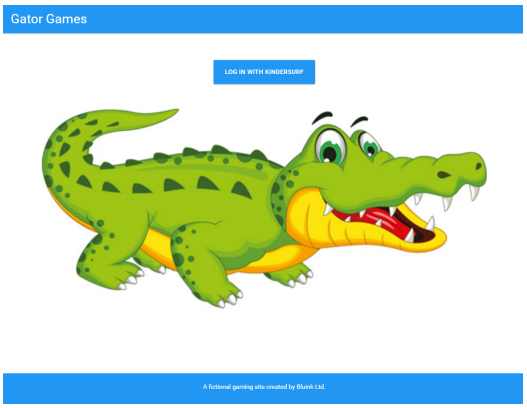
We designed the full interaction and intended functionality of the parent and child interfaces and implemented them as an improved user interface prototype for user testing.

The new interface was designed keeping in mind the needs and suggestion of the participants from the previous study as well as Bluink's requirements. Next, we discuss the requirements and the features of the prototype. Figure 4.4 gives an overview of the features and their hierarchy. Parents and children accessed this prototype on a mobile device.

4.3.1 Unique Identifier Mechanism and Optional Password

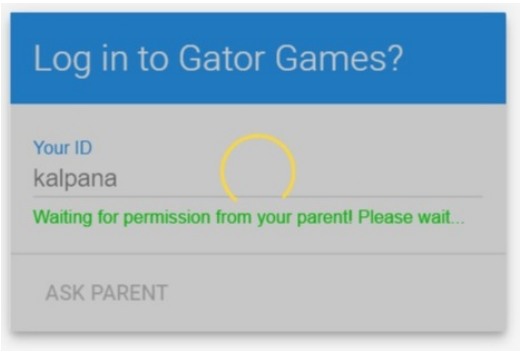
A child identifier is used to identify and link child's account to the respective parent account. We wanted to keep the child identifier unique, meaningful, and easy for children to enter. Also, we wanted all details of the identification mechanism to be entered on one screen and not require any additional hardware. We also added an optional password in order to secure the child accounts within the family, for example, to stop siblings from accessing each others' accounts.

Unique Child ID The child identifier is needed to identify the user to the server and link to the appropriate parent account. We have finalised the following scheme for the child identifier. It will contain two parts concatenated together as shown in Figure 4.5a:

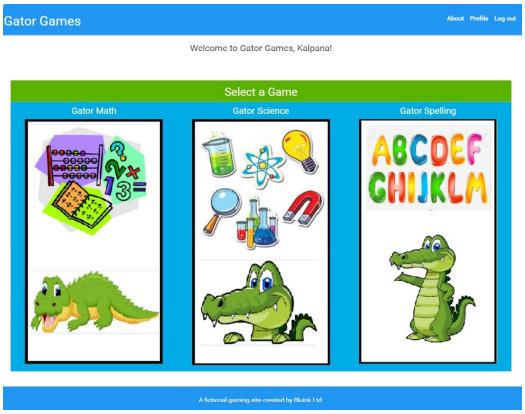


(a) Click Login

(b) Enter ID



(c) Ask Parent



(d) Parent Approved Access

(e) Parent Denied Access

Figure 4.3: Basic Communication Prototype - Interface for Gator Games

- Family username - When the parent installs the app and registers their first device, they must create a family username (minimum of two alphanumeric characters, and must be unique from existing accounts on the server). We keep the minimum low but place no upper limit (or could include a large one

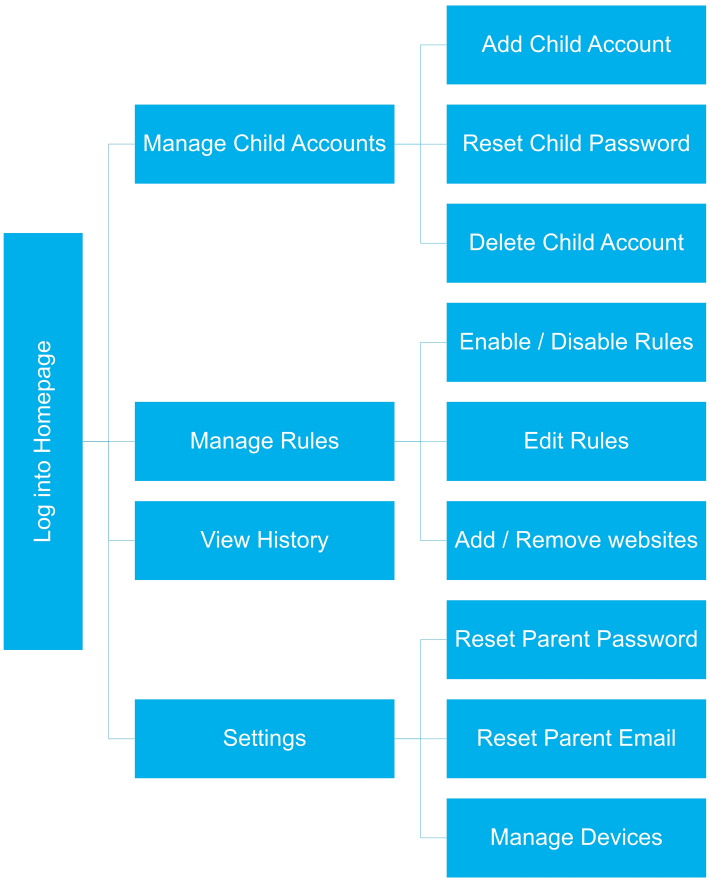
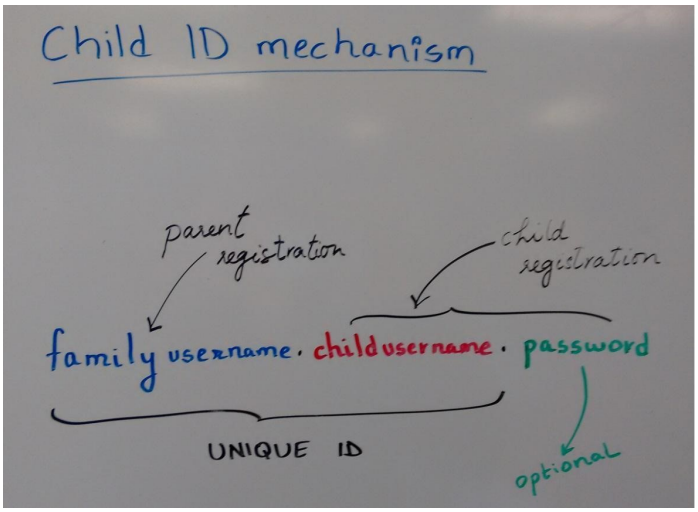


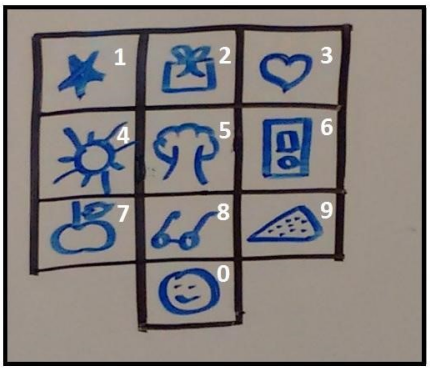
Figure 4.4: Overall Functionality

if technically required). There is no point in penalizing all the early families with a long identifier simply because eventually there might be a lot of users. The interface can suggest possible identifiers (such as phone number) but will not enforce one specific type of information. In our earlier study, some parents expressed concern over revealing too much information so we allow families to chose for themselves.

- Child username - When a child is registered, the parent chooses a nickname to identify the child. The same considerations as for the Family username apply. We let parents determine what makes the most sense for their children. Since the child username will never be used alone, uniqueness only applies within the family (e.g., there may be multiple children with 'Jane' as a username as long as they are from different families.).



(a) the Family username and the Child username forms the Unique Child Identifier.



(b) Password

Figure 4.5: Unique Identifier Mechanism and Password

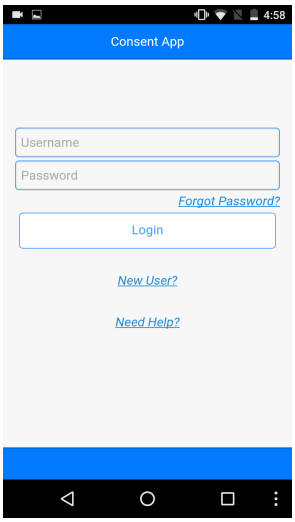
Optional Password - To keep accounts minimally secure from siblings or random online attacks, we provide an option for securing each account with a PIN/graphical password as shown Figure 4.5b. Given that parental permission is needed, the password is not strictly necessary to protect the website account. The password will be set from the Parent's device, when adding/editing child accounts.

The password is a grid with each square containing a digit and an image of an object. The minimum number of selected squares is set to two, with no upper limit. Given that the number of selected squares is variable, we need an explicit 'login' button (or pressing the Enter key) to identify when password entry is complete. Entry is allowed through mouse-clicks/taps or by entering the digits on a keypad/keyboard. From our first study, we found that young children preferred PINs and this type of object password, so combining the two seems reasonable.

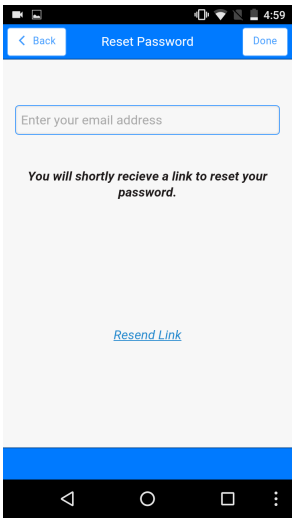
These passwords are relatively weak since they come from a small password space (and not mandatory). We have discussed including other secondary mechanisms to help protect the account, such as flagging requests from suspicious IP addresses or exhibiting unusual usage patterns. These will be part of future prototypes.

4.3.2 Parent Registration

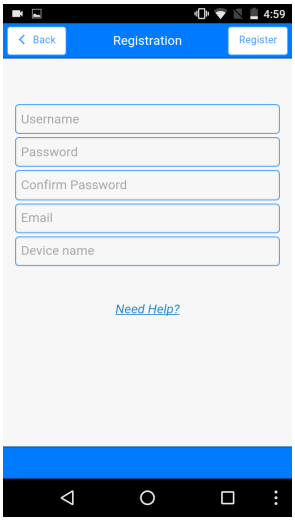
Parents have to install the app and register themselves as shown in Figure 4.7. The first parent would register themselves and their device to receive notifications, however the second parent (or the same parent using a second device) would use the existing family username to log in and register the second device.



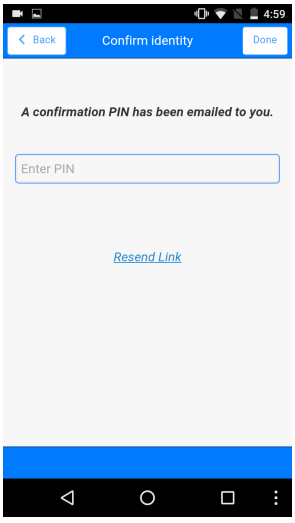
(a) Screen 1 - Login



(b) Screen 2 - Forgot Password

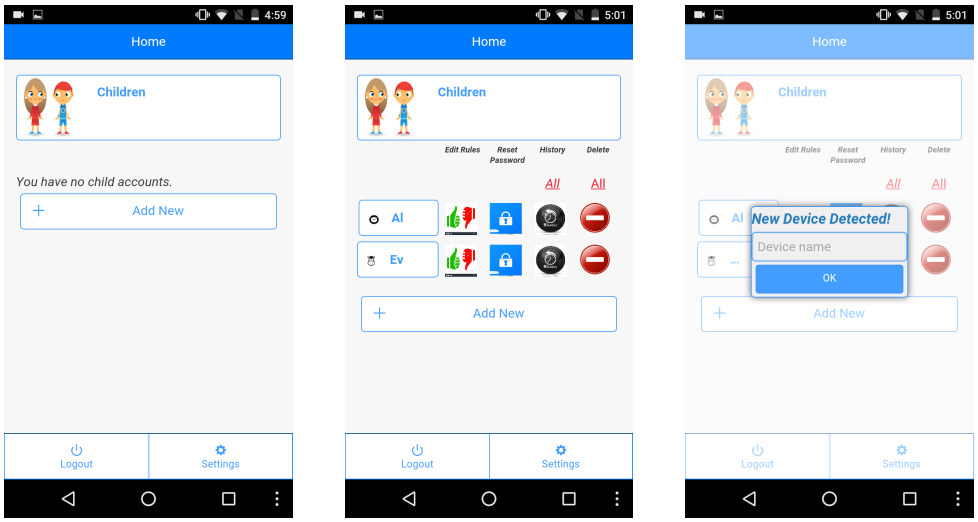


(c) Screen 3 - Register New User



(d) Screen 4 - Verify Identity

Figure 4.6: Parent Registration



(a) Screen 5 - Homepage (Navigated after registration)

(b) Screen 5 - Homepage (Registered User and Device)

(c) Screen 5 - Homepage (Login with new device)

Figure 4.7: Homepage

Screen 1 - Login: The parent logs in with their family username and alphanumeric password. Should the user forget their password, they can click on a hyperlink below the password textbox, which takes them to the Forgot Password screen (Figure 4.6b).

Typically, the app would remain logged unless the parent explicitly logs out, but to prevent children or others from modifying the settings, the password needs to be re-entered by the user on the Settings screen (Figure 4.11b).

To set up a new parent account, the user can click on 'new user' to reach to the New User for registration (Figure 4.6c).

Screen 2 - Forgot Password: The user enters the email address with which they registered. On clicking 'Submit', the user receives a link which will allow them to reset their password.

Screen 3 - Register New User: This page would allow a first time user to register themselves. Details such as the username (unique family username), password, email and device name are required. Once the user clicks register, they will receive a verification PIN via email.

Screen 4 - Verify Identity: When the user enters the verification PIN received, they are automatically logged in and shown the Homepage (Figure 4.7a).

Screen 5 - Homepage: After signing in, the user is taken to the Homepage. However, if logging on to a new device with an existing account, then the user has to provide a device name (which will be used as its identifier in the UI from this point onward) in order to access the Homepage (Figure 4.7c).

From the Homepage (Figure 4.7b), they can manage child accounts or their own settings (Figure 4.11a).

For child accounts, the parent can add a new child account (Figure 4.8a), apply website access rules (Figure 4.9), reset passwords (Figure 4.8d), view history (Figure 4.10), or remove an existing child account (Figure 4.8c).

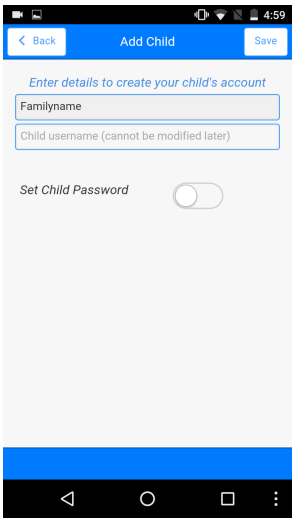
4.3.3 Add/Remove Child Accounts Workflow

After parents have registered themselves, they can add and remove child accounts.

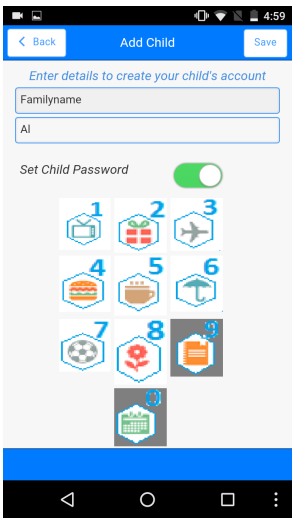
Screen 6 - Add Child Account: When the parent selects 'Add New' on the Homepage (Screen - 5), he is navigated to the Add Child Account screen (Figure 4.8a). Here, the family username is pre-filled. The parent enters a child identifier and can set a password for the child account. The password option is disabled by default. If a password is wanted, the UI area expands such that the password can be created and confirmed (Figure 4.8b).

After the parent is done creating the child account, they are navigated to Rules screen (Figure 4.9); and when 'Save' is pressed, they are returned to the Homepage (Figure 4.7b).

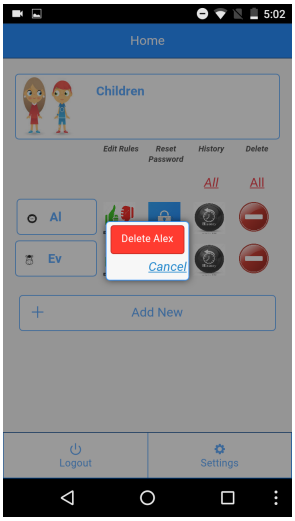
Pop-up on Screen 5 - Delete Child Account: Selecting the 'delete' icon on the Homepage results in a 'Confirm Delete' pop-up (Figure 4.8c), where the parent is asked to confirm their decision. Apart from an option to delete individual child accounts, parents can click 'all' above the delete icons to delete all child accounts.



(a) Screen 6 - Add Child Account (password disabled by default



(b) Screen 6 - Add Child Account (Password enabled)



(c) Pop-up on Screen 5 - Delete Child Account

(d) Screen 7 - Reset Password

Figure 4.8: Add / Remove Child Accounts

Screen 7 - Reset Password: Once a child account is created, parent can modify the password settings, i.e., enable/disable the password or reset it (Figure 4.8d; by clicking on 'Reset Password' icon from the Homepage.

4.3.4 Rules Workflow

A main feature of the app is the ability to set access control rules to automatically allow or deny child requests to visit websites at pre-defined times.

(a) Screen 8 - Rules (disabled by default)

(b) Screen 8 - Rules (enabled)

(c) Screen 8 - Rules (enabled - expanded)

(d) Screen 8 - Rules (Edit Rules)

(e) Pop-up on Screen 8 - (Add Website)

(f) Pop-up on Screen 8 - (Delete Website)

Figure 4.9: Rules

Screen 8 - Rules: Parents can set the access policy using a time-based grid that allows them to define what times the child can be automatically approved for login,

denied, or require on-demand permission. Rules are set per website.

If parents disable rules (Figure 4.9a), sites are set to ask for permission for each login attempt (visualized with grey bars). This is the default option selected. If parents enable rules, they select a mode: grey to always ask, green to auto approve, and red for auto deny; and then swipe over the grid cells corresponding to the desired times/websites them, i.e., apply rules.

As shown in the Figure 4.9c, the left column lists days of the week. When parents tap on a day, the UI expands and allows them to apply rules by time. Collapsed days visualize rules by compressing them into thin coloured lines (Figure 4.9b) summarizing the rules.

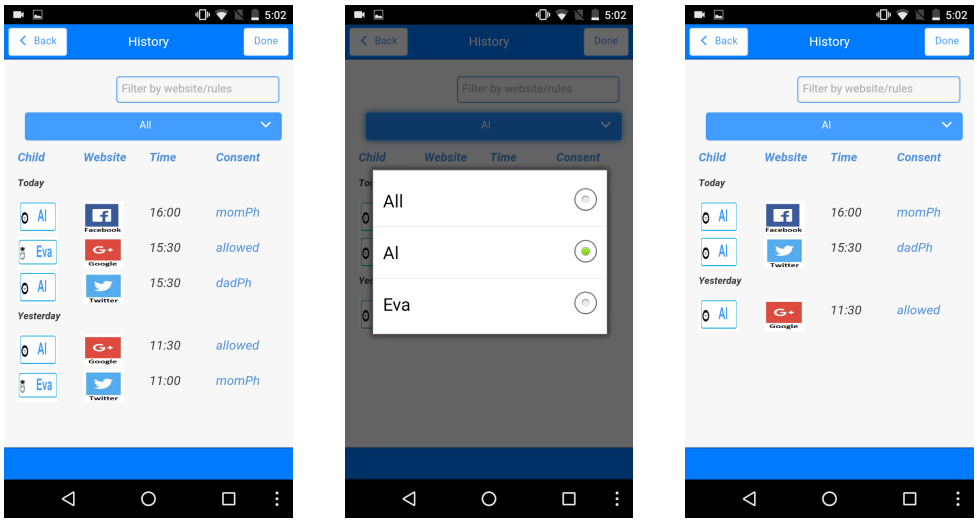
Screen 8 - Add/Delete Websites on the Rules: Parent can add websites by selecting the '+' icon, which results in an add website pop-up (Figure 4.9e). Long pressing on a website name results in a 'Confirm Delete' pop-up as shown in Figure 4.9f. The horizontal scroll would be enabled if more websites are added.

Since the app is based on OpenID Connect, only supported websites can be accessed. This facts limits the functionality of adding and removing websites. We can alternatively provide a dropdown box of supported websites from which they can select.

Screen 8 - Edit Rules: Parents navigate to this page (Figure 4.9d) to enable/disable rules, modify existing rules and add/delete websites, by clicking on 'edit rules' from the Homepage.

4.3.5 History

Screen 9 - History: Parents can view previous approved logins for their children. The history is accessed from the Homepage, by selecting individual (Figure 4.10c) or all child accounts (Figure 4.10a). If the parent clicks on a child's name on the history page, a list containing all users is displayed (Figure 4.10b). The parent can select whose details to view.



(a) Screen 9 - History (all accounts)

(b) Screen 9 - History (drop-down)

(c) Screen 9 - History (individual accounts)

Figure 4.10: History

4.3.6 Settings

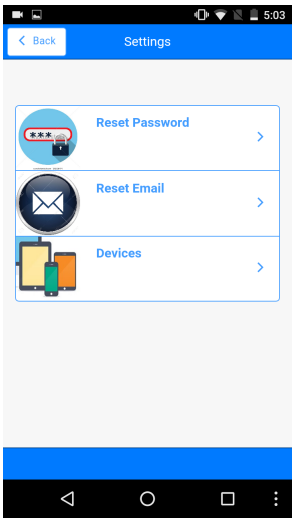
Screen 10 - Settings: The Settings screen (Figure 4.11a) allows parents to reset their own password (Figure 4.11c) or update their email address (Figure 4.11d). It also enables parents to add or remove devices. However, parents must re-enter their password (Figure 4.11b), to perform any action on the Settings screen.

Screen 13 - Devices: Existing devices are listed (Figure 4.11e) by name with options to enable, disable or delete existing ones. The default device cannot be deleted. A note informs parents that new devices can be added by logging in with their family ID from the new, non-registered device.

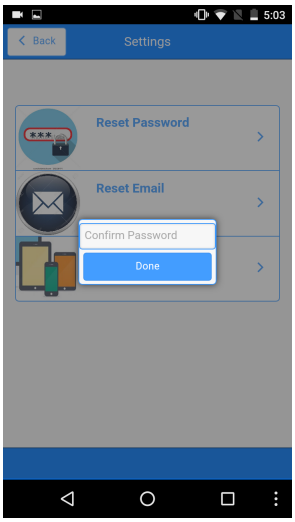
4.3.7 Authentication Process

The authentication process is demonstrated in the KinderSurf - Basic Communication Prototype, although the user interface is minimal (Figure 4.2 and 4.3). We include the missing features in our user interface prototype.

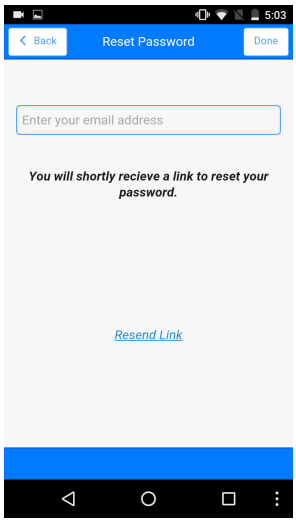
Screen 14 - Child Request Access: The child enters their unique username (familyusername.childusername) and password (if one has been set), and can add an



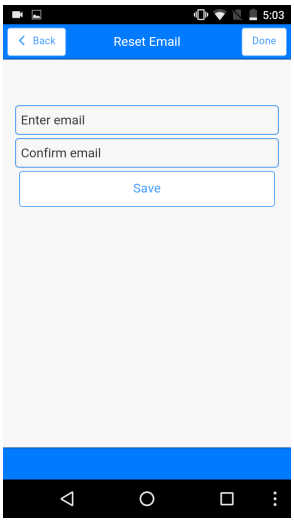
(a) Screen 10 - Settings (all options)



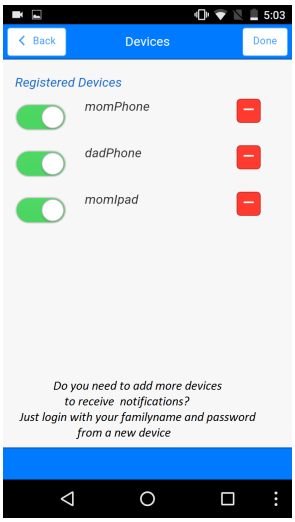
(b) Pop up on Screen 10 - Confirm Password



(c) Screen 11 - Reset Password



(d) Screen 12 - Update Email



(e) Screen 13 - Devices

Figure 4.11: Settings

optional message along with their request for authorization, as shown in Figure 4.12a. Messages may be typed or selected from emojis [3] (preset visual messages).

Screen 15 - Parent Response: When the child requests login, the parent receives a notification on their device Figure 4.12b. The notification includes the website that

[3]These are not the finalised emojis; we will be looking into royalty-free emojis at a later stage.

the child wishes to visit and the child's message (if applicable). The parent can either approve or deny the child's request, and can add an optional message of their own. The parent's response is displayed to the child. If the parent grants access, the child is logged into the webpage after displaying the approved login status (Figure 4.12c). If the child has been denied access, a failed login status (with the parent's message, if applicable), appears (Figure 4.12d).

When the parental app is installed and registered on multiple devices, push notifications are sent to all devices. The first response is accepted and the request is removed from other devices.

4.4 Infrastructure

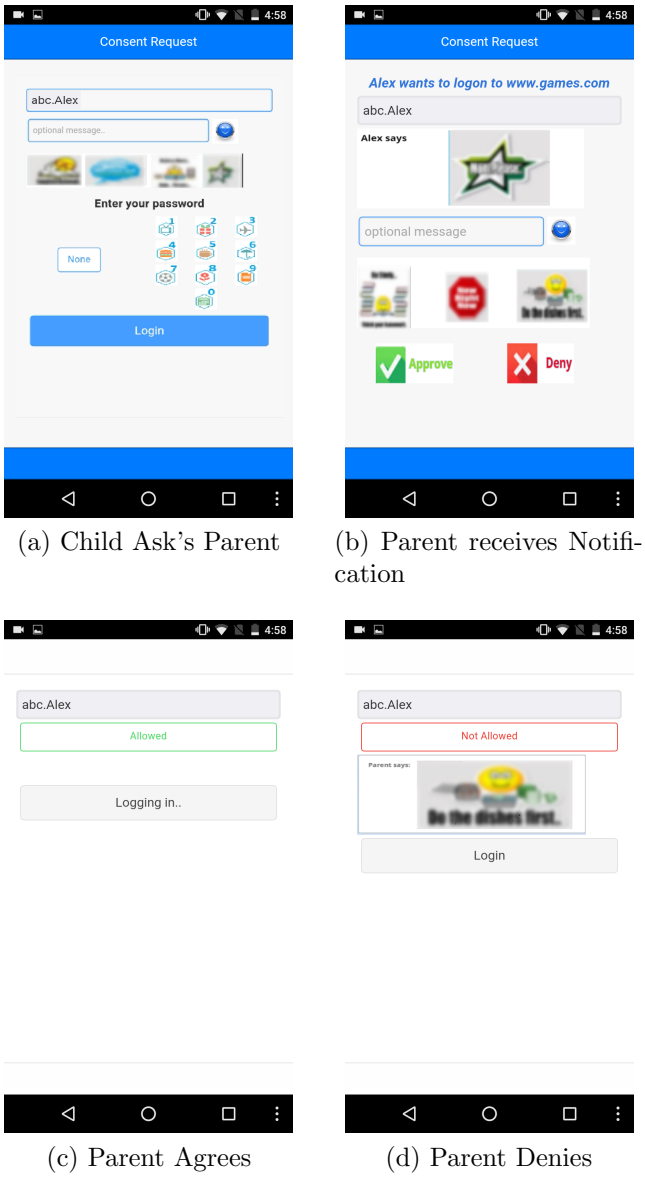
As mentioned earlier, the prototype is based on OpenID Connect technology as the authentication mechanism. A child requests consent to log in to a supported (Relying Party) website via a (User Agent) browser. The unique (Open ID) identity of the child is used to lookup their parent's device. The connection between the child's accessed website and parent's device is established via Bluink's Relay Service. Furthermore, push notifications notify the parents and the child's authentication request can be handled.

Bluink is actively developing the infrastructure to support the app and is currently working on the following modules:

- *OpenID Provider* – A webservice that would not only manage parents, their children and registered devices but also enable client - third party web applications to use KinderSurf authentication as a service.

- *Authorization Endpoint* – Sample webpages where the user is authenticated and secure connection initiates. This Relay connection between the registered device and authentication service is implemented via JavaScript.

- *Smartphone App* – The app that would enable parents to view and modify their settings, manage their children's accounts and associated access policies. The app receives push notifications enabling parents to provide authentication consent remotely.



(a) Child Ask's Parent

(b) Parent receives Notification

(c) Parent Agrees

(d) Parent Denies

Figure 4.12: Adding Communication in Notifications. Image blurred due to copyright.

- *Other Services* – The push notification service, sends authentication consent requests to the parent devices and receive their response. The Relay service enables connections and communication between the Authorization Endpoint (accessed webpage) and the parent's authenticating device. The App would need access permissions to use these services.

The workflow of the prototype is shown in the Figure 4.13. However, this is not the finalized version, as some restructuring is possible.

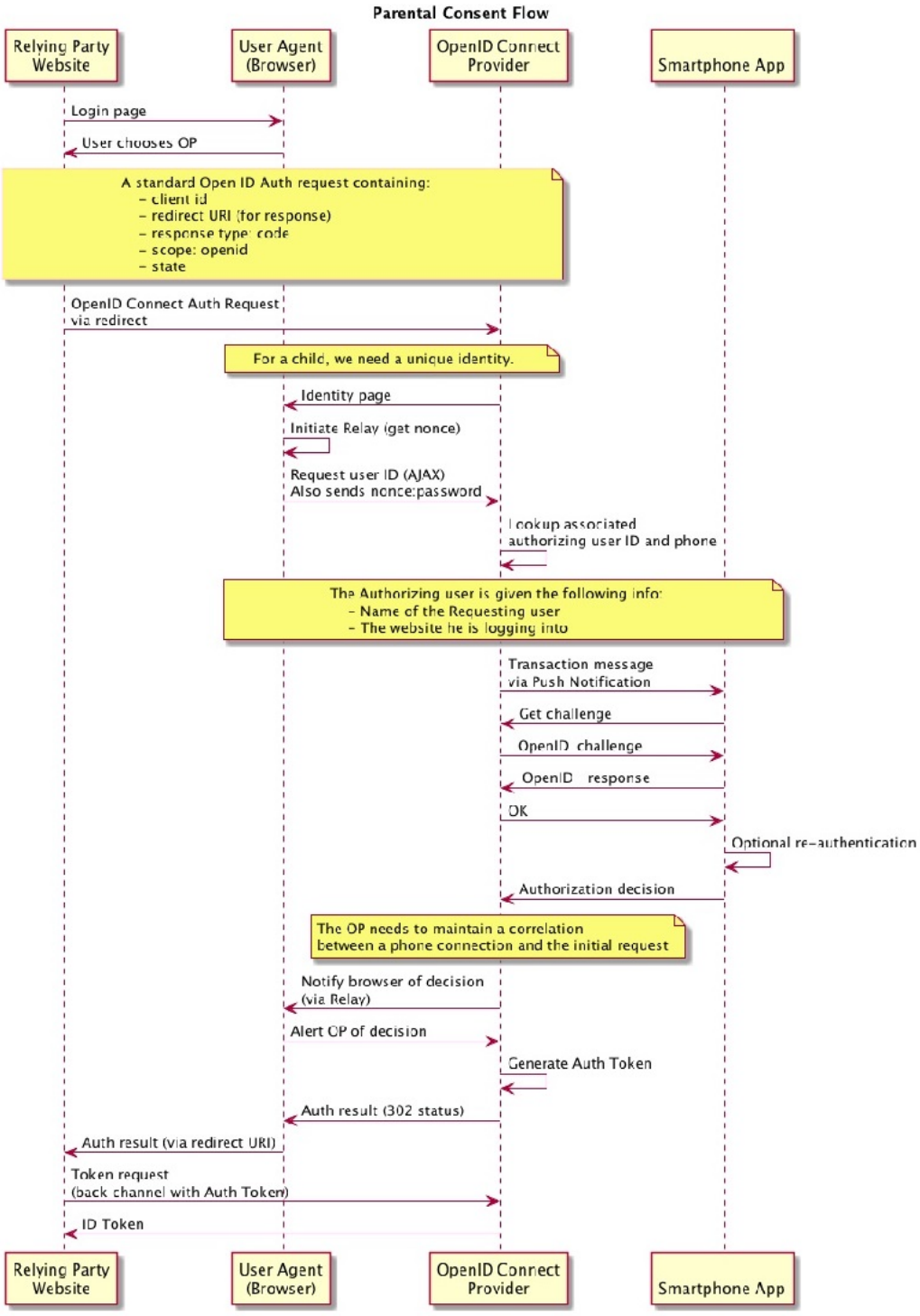


Figure 4.13: KinderSurf Workflow [47]

4.5 Summary

This improved prototype details the features of the app and allows for user testing. We are particularly interested in the complex interactions (for example, the rules page). We will conduct a user study to gain feedback from parents and children.

Chapter 5

User Study of KinderSurf

This chapter focuses on the user study for the improved password manager prototype – 'KinderSurf'.

The user study was conducted to gauge the usability as well as acquire feedback regarding user preferences, from both parent and child participants. The main aim was to assess the aptness of this prototype and thereby ascertain the areas that require any further development.

This research was approved by Carleton's Research Ethics Board-B. The study protocol is same as the previous study (described in Section 3.3). The interviews took place at a public location of the parent's choice and lasted approximately 60 minutes. The parent-child dyads sat through in-person individual sessions with the experimenter. The children performed the tests first, and then were offered some activities while the parents completed their session.

The parent-child dyads followed the same general process:

- A pre-test interview: We queried participants about their demographics and asked questions about their current use of passwords and single sign-on.

- Prototype testing: Parents and children were demonstrated the overall working of the KinderSurf - Basic Communication prototype, via the 'KinderSurf' app (Parent Interaction) and 'Gator Games' website (Child Interaction) briefly. They then interacted with the KinderSurf - User Interface prototype based on the tasks assigned and suggested preferred changes. They were encouraged to comment while interacting with the prototype. Tasks involving the Basic Communication prototype were done with the parent and child working together. Tasks involving the User Interface prototype were done individually. However, in some instances the parents chose to remain with the child even during the individual tasks.

- Post-test interview: We conducted a brief interview pertaining to their experience with the prototype and preferences.

We explained the overall functionality of the KinderSurf - Basic Communication prototype via the 'KinderSurf app' on an iPad (parent's view) and 'Gator Games' website on a laptop (child's view). The iOS and web versions of the Basic Communication prototype, designed for parent and child respectively, were developed by our collaborators at Bluink [1]. The participants also interacted on a smartphone with the password manager app (KinderSurf - User Interface prototype), that we developed via Appery [2] using Html and JavaScript.

5.1 Study Protocol

The study protocol comprised of the following steps. The same general procedure as in the first study was used (Section 3.3). We describe the steps that differed.

1. Greeting.

2. Consent process.

3. Session with Children

   (a) Children answered pre-test interview questions (Appendix C) and we audio recorded their responses.

   (b) Children were explained the functionality of the prototype and interacted with it to complete the following tasks:

      i. Gator Games login – Children click "Log in with KinderSurf", enter the ID provided by their parent and then click "Ask Parent". They witnessed that their parent gets a notification and that they are logged in if their parent approves the request. (Prototype: KinderSurf - Basic Communication - Child Interaction)

[1] `http://www.bluink.ca/`
[2] `https://appery.io/`

ii. Send Consent Request – Ask parents for permission to sign-in by entering a username, an optional message, and an optional password. (Prototype: KinderSurf - User Interface)

(c) After the tasks, children answered post-test interview questions (Appendix C) about their opinion of the prototype and their password and messaging preferences.

4. Session with Parents

(a) Parents answered pre-test interview questions (Appendix D).

(b) We explained the functionality of the prototype, then parents interacted with it to complete the following tasks. The tasks are broken into several micro-tasks to make sure we got feedback on all aspects of the prototype.

i. KinderSurf login approval – Parents registered with the provided email address and logged in. Furthermore, they provided their child with an ID and responded to the notification received when the child tried to log in from the web. (Prototype: KinderSurf - Basic Communication - Parent Interaction)

ii. Respond to Consent Request – Parent had to select either 'Approve' or 'Deny', accompanied by an optional message, in response to the push notification (consent request) received. (Prototype: KinderSurf - User Interface)

iii. Register New User – Parents were expected to register themselves as a new user by entering their family username, password, email address and a device name. After registering, they had to enter a PIN emailed to them to verify their identity, and navigate to the homepage. (Prototype: KinderSurf - User Interface)

iv. Create Child Accounts – Parents created an account for their child by setting up a child username and optional password. They were asked about their preference on whether to use a password for their child; and on using their child's realname versus nickname as a username. (Prototype: KinderSurf - User Interface)

v. Enable/Disable Rules – Parents were asked if they preferred to set up rules or receive notifications of every login request from their child. Parents enabled and disabled rules. (Prototype: KinderSurf - User Interface)

vi. Apply Multiple Rules for one day – After enabling rules, parents added multiple rules in one day for a website. (Prototype: KinderSurf - User Interface)

vii. Apply One Rule for an entire day – Parents created one rule applicable to an entire day. (Prototype: KinderSurf - User Interface)

viii. Login as Second Parent – At the login screen, parents were asked to assume that they were the second parent whose device is not yet registered. They logged in with the existing family username on a new device. (Prototype: KinderSurf - User Interface)

ix. Enter new device name – When they logged in from a new device as a second parent, a pop-up asked for a device name before letting them proceed to the homepage. (Prototype: KinderSurf - User Interface)

x. Reset Password – The parents reset the password for a particular child on the homepage. On the reset password screen, they disabled the password if it was enabled or vice-versa. (Prototype: KinderSurf - User Interface)

xi. Edit Rules - Parents clicked the edit rules icon on the homepage, and, on arriving at edit rules screen, change an existing rule. (Prototype: KinderSurf - User Interface)

xii. Add Websites - From the rules screen, they added a new website by clicking on the "+" icon near the website names. (Prototype: KinderSurf - User Interface)

xiii. Delete Websites - Parents deleted an existing website by long pressing the website name and then confirming delete action. (Prototype: KinderSurf - User Interface)

xiv. View History for all children – The parent were asked to view login

attempts of all child accounts. (Prototype: KinderSurf - User Interface)

xv. View History for one child – From the history screen, the parents navigated to view login attempts of individual child accounts via a dropdown list. (Prototype: KinderSurf - User Interface)

xvi. Delete Child – Parents deleted individual child accounts from the homepage and confirmed the action. (Prototype: KinderSurf - User Interface)

xvii. Update Settings – Parents changed the email address associated with the parent account via the setting screen, confirmed their identity, and clicked 'Update Email'. (Prototype: KinderSurf - User Interface)

xviii. Disable a Device – Parent navigated to the devices screen and disabled a device. (Prototype: KinderSurf - User Interface)

(c) Parents answered post-test interview questions (Appendix D).

5. Wrap up.

5.1.1 Participant Demographics

Ten parent-child pairs (20 participants) participated in the study. Five of the pairs had also participated in the previous study giving them the ability to compare the two prototypes, while the new participants allowed us to assess the learnability for first-time users. Recruitment was done via invitations on social media, posters, and through our network of acquaintances. A necessary condition for the pair to participate was that the child be an online user within the age of 7-11 years [3] and be accompanied by their parent or guardian.

Among the participants, we had seven girls and three boys (mean age of 9.4 years old), from grades 2 to 7 (mean grade 4.6); two children were home-schooled. They were accompanied by six mothers and four fathers (all falling in the age group of 30-50 years); two parents were single-parents. Table 5.1 details the participant demographics.

[3]However, we included one child who had just turned 12 years old because he was a part of our previous study.

P#	Child Age	Child Grade	Child Gender	Parent Gender	Parent Age	Parent Occupation
1	8	4	f	f	34	bank teller
2	7	2	f	f	31	business administration
3	10	6	f	m	38	software developer
4	11	5	m	f	40	customer service
5	12	7	m	m	35	manager
6	7	2	f	f	34	computer programmer
7	8	2	f	f	37	education administration
8	10	5	f	m	45	engineer
9	11	6	m	m	50	marketing
10	11	7	f	f	44	educational assistant

Table 5.1: Participant Demographics

5.1.2 Data Collection

As with previous study (Section 3.3.2), data was collected through audio recording and written notes. The audio recordings were transcribed and analysed by the experimenter.

We classified the data in five general categories:

1. Demographics: We recorded gender, age, grade and parent's occupation.

2. Online knowledge and behaviour: We derived this data from interview questions covering the knowledge of passwords, children's online habits, current permission habits.

3. Participant preferences: Participants indicated their preferred choices for usernames, rules, passwords, and communication options.

4. Tasks accomplished: We recorded if the participants completed the tasks without help, completed them with some help, or did not complete them.

5. Prototype feedback and suggestions: Participants provided their feedback on the prototype and suggested improvements.

5.2 Results

Based on our data classifications, following are the results from each category.

5.2.1 Demographics

Table 5.1 reflects the basic demographics of participants. We had participants of various backgrounds.

Participant	'What is a password?"
Child-1	"It is used on a phone."
Child-2	"So nobody gets into your accounts"
Child-3	"A password is something that is a combination of pictures, or numbers that you use or patterns that you use to make sure that everything you need to keep secure is secure. "
Child-4	"It is to keep something personal things safe from other people."
Child-5	"Something that locks your account information."
Child-6	"We use not a phone but on a computer."
Child-7	"protect device."
Child-8	"Something that you can protect with your own decision of what you want your password to be And you can protect, for example you can protect your iPad, nobody can get into it except for the people that know your password."
Child-9	"Something to allow you to access a certain thing; so if you have a password called computer you will have to enter computer to access something."
Child-10	"It is something that keeps an account on a website safe that no one else can use it."

Table 5.2: Children's Description of "Password"

All the participating children were aware of the term 'password', and could explain it to varying degrees (Table 5.2). We initially found that children having a parent in the engineering or science fields were able to define the term more thoroughly. For example, software developer's child said, "A password is something that is a combination of pictures, or numbers that you use or patterns that you use to make sure that everything you need to keep secure is secure". However, this child was also older, so it is unclear which factor had a bigger impact. We observed a difference in thinking and complexity of responses between the older (above 10 years) and younger

(7-8 years) children. Even though the majority of our data suggests a relationship between children's online knowledge and their parent's occupation, we cannot make any definitive claims due to our small sample size and the confound of age.

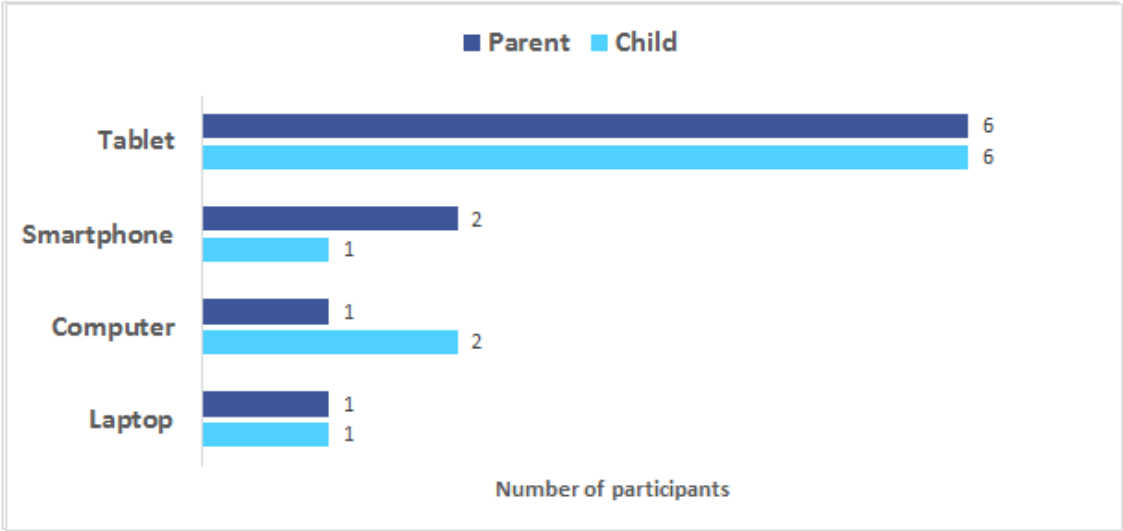


Figure 5.1: Most frequently used device for children as reported by each group.

We asked participants which device children use the most. As shown in Figure 5.1, children used tablets most frequently.

5.2.2 Online Knowledge and Behaviour

Nine children said they had a password; but as we proceeded with the tasks, we discovered that three children (aged between 7 and 8) did not understand either passwords or being online. On probing further, we found that the parents of those children either had the children auto-login or entered the password for them.

Children had fewer than five accounts, except for one child who had 10-15 accounts. Five children said they share passwords with siblings, while seven parents acknowledged siblings sharing passwords. Three parents and three children clarified that the children only shared passwords for games and common devices. Moreover, when asked if all siblings had the same rules for going online, six children and five parents agreed.

Six children said they need permission to log in to websites, but only two parents agreed. This discrepancy appears to be due to the fact that some children do not need permission to log in to known websites, but required permission to use a device, to make online purchases, or try something new. When children were asked to whom they ask permission, six children said mother, three said father while one child said both parents. Furthermore, all parents claimed they knew if their child was online irrespective of whether they asked for permission. Figure 5.2 displays child responses and Figure 5.3 shows parents' responses about their children's habits.

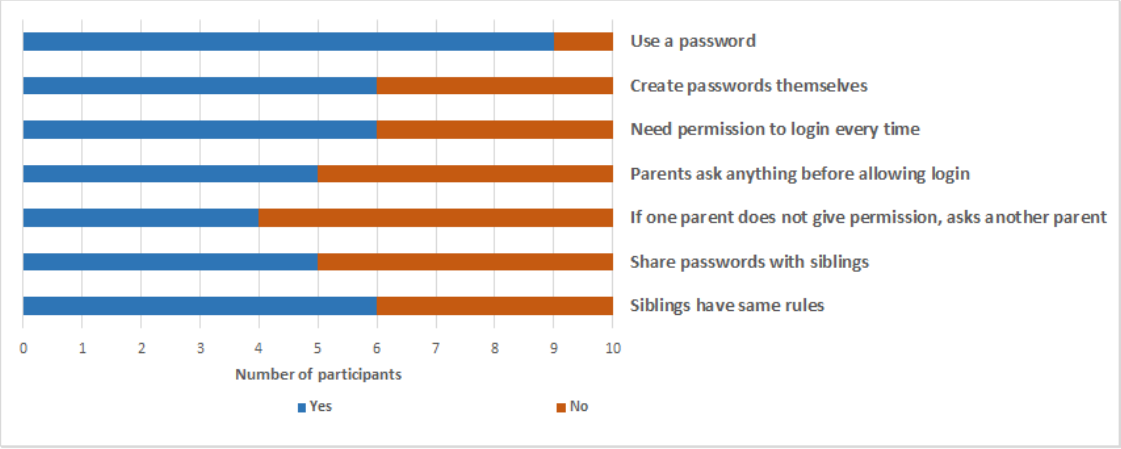


Figure 5.2: Children's reported Habits

5.2.3 Participant Preferences

A new password type combining PIN with graphical password was used in the prototype and participants gave their opinion of it. Six children liked the PIN + graphical combination, but four still preferred text passwords. Moreover, eight children said they would use a password while two preferred having none. Seven parents preferred the new password scheme and wanted to include a password for their child; the remaining three preferred text passwords and would not use a password for their child's account. These parents said a password was either too difficult for the child to remember or it was unnecessary since parents could approve/deny login requests. Figure 5.4 summarizes these password preferences.

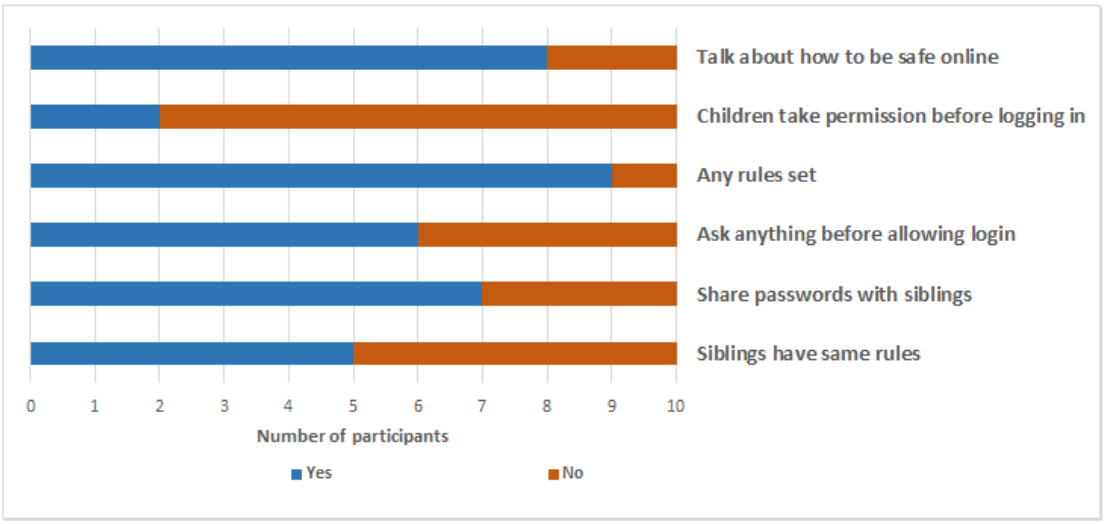


Figure 5.3: Parents' reporting of Children's Habits

Figure 5.4: Password Preferences

The KinderSurf User Interface Prototype offered the ability to add optional messages when requesting consent for login. Figure 5.5 shows participants' preferences relating to messages. Five children and seven parents said they would use messages.

Six parents and six children voted for typing their own message versus using emojis. A common reason for using text was because emojis offered limited options and they felt it was better to write in their own words. The parents of younger children mostly preferred emojis as they felt their children would find it difficult to type a message. Eight parents preferred using only a single message exchange, while two requested conversation-like communication because they felt the child would text them anyway from somewhere else to convince them to grant access.

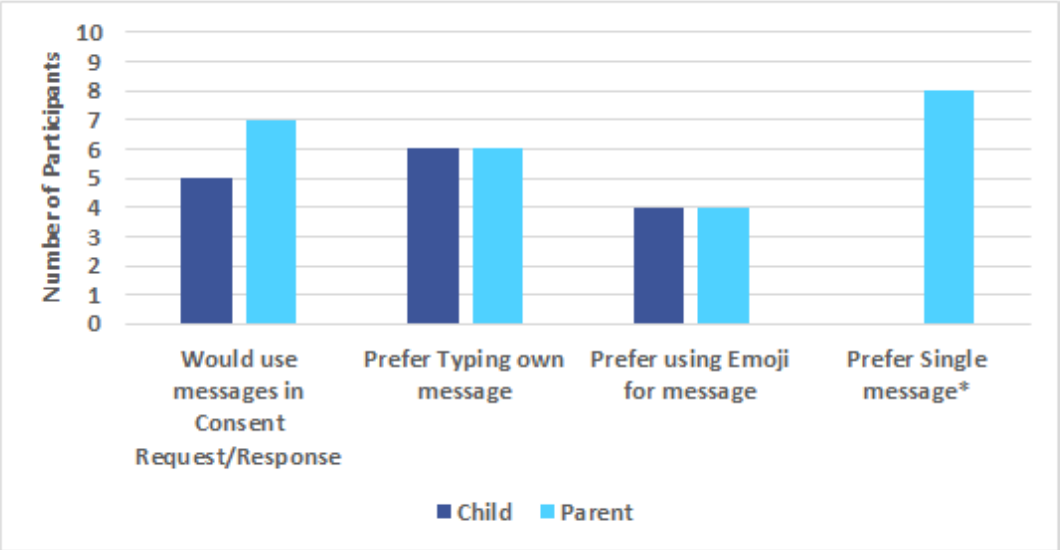


Figure 5.5: Message Preferences *only parents answered this question.

We also inquired about a few other design decisions from parents. Three parents would use the child's real name as the child's ID, four would use a nickname, and the others did not express a preference. All parents wanted a feature to copy rules across child accounts. Moreover, eight parents wanted to see approved as well as denied login requests in the history while two wanted to view only approved logins.

5.2.4 Tasks Accomplished

All participants successfully completed the login tasks. The majority of children successfully completed the 'Send Consent request' task. As mentioned earlier, three children ages 7-8 years old could not complete the task because they were not very

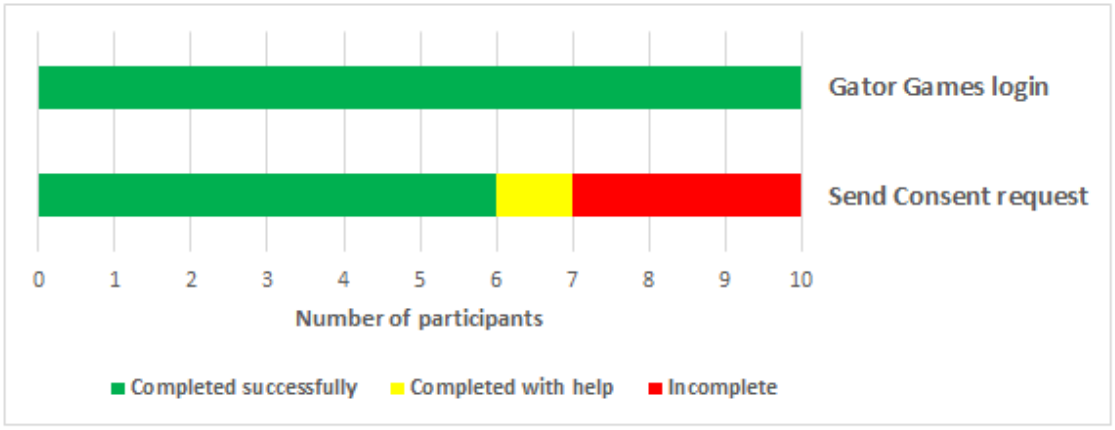


Figure 5.6: Completion results for Child Tasks

Figure 5.7: Completion results for Parent Tasks

familiar with how to log in. The parents informed us that they either enter the password for them or the children are auto-signed in. Thus, they log in but are not very aware of it. Children's task performances are summarized in Figure 5.6.

Parents' task performances are summarized in Figure 5.7. Parents completed the majority of tasks successfully. Common errors were logging in without creating a new user ('Register New User' task), re-registering when logging in as another parent ('Login as Second Parent' task) and returning to the homepage rather than using the dropdown to view the history for an individual account.

The majority of parents got confused in the tasks involving the rules screen. Eight parents did not turn rules on ('Enable/Disable Rules' task) before trying to apply them. Also, they faced difficulty trying to figure out how to apply multiple/same rules and add/delete websites. The rules screen is the most complex, has a lot of information, and the prototype implementation had limitations which affected usability. In the majority of tasks with errors, participants were seen clicking labels instead of icons to carry out tasks. For example, to create rules, they would tap on the website name and weekday, expecting the intersection to become coloured. We saw similar label confusion on homepage, where they clicked on a child name rather than the corresponding icon.

5.2.5 Prototype Feedback and Suggestions

We asked parents three Likert scale questions relating to their use of the prototype. Most would use the app and its rules feature, rather than approving individual requests; as shown in Figure 5.8.

Parents responses' during the post interview session are mentioned below. Six parents favour the proposed password manager prototype compared to their existing authentication method for children. All parents would want requests sent to their mobile phone; six would rather use an Android app, while four selected an iOS app. One participant would want the app installed on more than five devices. The remainder would install it on between one and three devices. The parents reported that children would use the app to log in to between one to ten websites (mean = 5.6). Most parents would want either parent to approve consent requests. Parents were also willing to pay for this service as shown in Figure 5.9.

An interesting suggestion was made by a parent who requested an exception to rules shortcut. For example, if they (parents) created rules for Monday to deny a

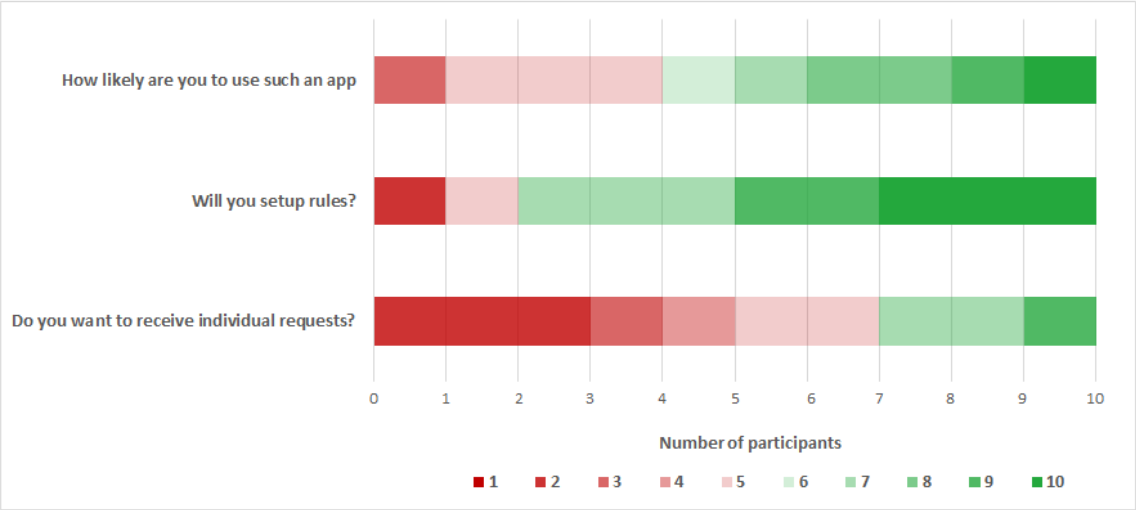


Figure 5.8: Parent Likert scale Responses; 1 = most negative, 10 = most positive

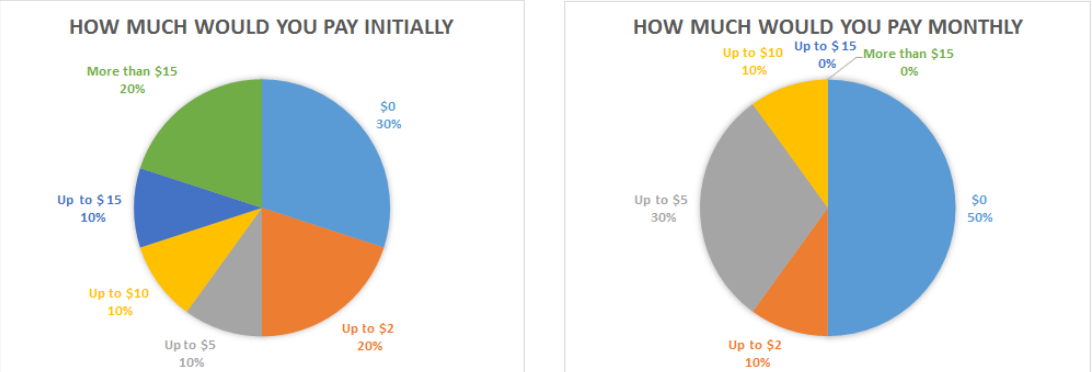


Figure 5.9: Price Preference for the Service

website but wanted to allow it only one time; as an exception, they did not want to have to modify rules. Another parent asked what to do if the parents are separated and did not want to share a family password. We received a few other suggestions in this user study. Parents suggested using a garbage can icon for delete instead of long press and requested personalized emojis. Almost everyone found the rules page confusing; one parent suggested having radio button to select rules at the top and bottom to reduce scrolling. One parent wanted to see when the child logs out as well, but this is not technically feasible since control is passed to the website after authentication.

5.3 Discussion

This section discusses our findings of this user study.

Comparison with previous study: We saw fewer discrepancies between parent-child interview responses in this study. This is likely due to the fact that most parents sat in close proximity to their children and could hear them, so modified their responses accordingly. Also, since half of the participants were from the previous study, there was less mismatch between the users' mental model and system model.

Design Improvements: We found that many parents got confused on complex pages due to user interface design choices. For example, the rules page interaction was not intuitive. Our next prototype will use a touch slider for selecting times and we will make the labels interactive. Also, the delete icon was available on all pages, except for delete website function on rules page, which used a long press on the website name in order to delete it. Such inconsistencies in the design led to usability issues. We have noted such design flaws and will rectify them.

5.4 Summary

The results reflect that parents would use the KinderSurf app and would pay for this service. A parent inquired, "When would you be releasing this service? I want to use it." Parents preferred setting rules rather than approving individual requests, despite the fact that the page was initially confusing to them. After learning to use the app, they really liked it. Some parents said they would even want to use it with their older children. In future work, we will improve this prototype to be released as a fully functional app.

Chapter 6

Discussion and Conclusion

In this thesis, we focus on child authentication via a password manager that is managed by parents. We started with our 'Keep A Secret' prototype, a parent-managed password manager for children. On the next iteration, we designed 'KinderSurf', a parental consent authentication mechanism based on the OpenID concept.

6.1 Mental Models

OpenID provides various benefits over passwords [58]. It helps in password reduction, by letting the users sign-in to multiple accounts with only one pair of credentials. It also saves users time because they do not need to create new accounts and remember many individual passwords.

When we asked parents if they knew about Single Sign-On/OpenID, many seemed confused. However, when we narrated a use case scenario to them, they were familiar with it. Many, said they currently sign in to websites via Gmail and/or Facebook. On probing further, we found that users have no mental model of how SSO/OpenID authentication works. They asked questions and seemed curious when interacting with the 'KinderSurf' prototype. When carrying out a task, parents inquired about the consequences. For example, a parent asked "How will my child login to websites? Will they use this password to sign in?" when trying to create a child account i.e., an OpenID for the child. However, once they understood the working of the prototype, they had positive opinions of it. Thus, if we deployed KinderSurf, we would need to help users build their mental model of the system by making the interface interactive, intuitive and easy to learn. We could also add a quick tour and guide them initially, and explain at a high-level how the components work together.

6.2 Perception of features

Our initial goal was to focus primarily on helping to manage the burden of passwords. Parental controls were a secondary feature in our initial design. On the contrary, we found that parents focused more on parental control/monitoring, and less on the password manager features during our user-testing. This is interesting given that most families discussed problems with their children's passwords and revealed coping strategies for dealing with the fact that children forget passwords and locked themselves out of accounts. Several parents managed the authentication process for their younger children. It is possible that parents are content with their current coping strategies and saw the parental control as a new tool for a task that they could not currently accomplish. Our lab testing only had children logging in to one website (although parents saw multiple websites on Rules screen), so this may not have fully conveyed the benefits of password management. Alternatively, it may be that the prototypes took away the burden of passwords and so parents could focus on parental control as a beneficial additional feature.

6.2.1 Methodology considerations

We reflected on our experiences during user testing with parent-child pairs and summarize some of our insights. Ideally, the child and parent portions of the user testing session would be separate since in real life they would not be co-located during use. However, conducting lab testing with young children can be challenging and we wanted to make sure that children were comfortable. In our methodology, parents remained in close proximity to their children. However, there were instances when parent sat directly with the child and would unintentionally start assisting them during the session. Also, if the child did not know an answer, they asked their parents what to answer. This also impacted parents' responses in their session as they already knew what the child answered.

We found that children were more engaged when interacting with the prototype versus when interviewed. While carrying out a task, they had a reference point and context for their comments, compared to the interview where they were asked questions about past or future situations they had to imagine or recall. Also, the

children seemed more comfortable when the session involved their parents interacting as well.

Furthermore, we recommended that session with children be short and have very specific tasks. Our tasks for children were very specific and short and this was effective. However, our interview sessions were sometimes longer, and we found that the children very eager to complete the study and go do the drawing activity instead of answering questions. Also if a question got repeated, they often got confused as to why was the question being asked again and tried to recall their previous response. Other times, they were unsure about a question and they looked to their parents for help. Thus, we advise that extra care be taken with the wording of questions and tasks when working with children.

We also found inconsistencies in the participants' responses if questions were repeated. For example, parents were asked if they would enable the rules or passwords while they were directly interacting with the prototype. In the post-interview session, they answered the same questions. Their responses were not always same, sometimes participants changed their mind during the study. It may be possible that they initially did not have a full mental model of the prototype, but got familiar with it during their interaction. In case of any inconsistency, their post-questionnaire answers were considered final.

6.2.2 Evaluating KinderSurf

As mentioned earlier, passwords still exist despite known problems, because alternatives lack in terms of deployability [10]. Password managers have their own usability issues and are sometimes even hard for adults [16]. Bonneau et al. [9, 10] have previously proposed the "UDS" (usability-deployability-security) framework for evaluating web-based authentication schemes. We use their framework to assess KinderSurf. Their framework has 25 criteria deemed important and the original authors compared 35 schemes based on these criteria. A main finding is that no scheme fully addresses all criteria and, thus, the ideal scheme depends on the context of use and threat model. OpenID has already been evaluated and results show that generally it has substantial benefits over passwords in terms of usability as well as security. Since

KinderSurf is based on OpenID, our discussion focuses on criteria where there were differences. Items in italics represent criteria defined by Bonneau et al. [10].

We first examine the usability benefits. KinderSurf uses an optional password, making it potentially *Memorywise-Effortless* except that children must remember a username. It is potentially *Scalable-for-Users* since one OpenID works for all supported accounts as long as websites choose to implement support for it. KinderSurf is dependent on parents' authorization device (usually a phone), but that can be mostly eliminated by creating rules, thus the *Nothing-to-Carry* criteria is met for children and partially for parents. The child sends consent request by entering their userID id and clicking 'Ask Parent' and the parent responds by clicking 'Approve' or 'Deny'. Users can be authenticated via the click of a button since other fields are optional, thus we can call it *Physically-Effortless* for children. It is relatively *Easy-to-Learn*; although some new users hesitated to try it, they exclaimed that it is easy to use once they know what it is. OpenID was already rated [10] positively on the *Easy-to-Use*, *Infrequent-Errors* and *Easy-Recovery-from-Loss* criteria. Given this, we can say that KinderSurf adds usability benefits to OpenID.

Secondly we examine deployability benefits. KinderSurf (like OpenID) offers benefits of being *Accessible, Negligible-Cost-per-User, Browser-Compatible, Mature and Non-Proprietary* but is not *Server-Compatible*. As mentioned [10], OpenID is favourable in terms of deployability, but lacks server compatibility because websites must make infrastructure changes to accept user authentication through OpenID.

Lastly we examine the security benefits. OpenID potentially provides many security benefits (*Resilient-to-Throttled-Guessing, Resilient-to-Unthrottled-Guessing, Resilient-to-Targeted-Impersonation and Resilient-to-Physical-Observation* [10]) by reducing possible attacks to only the ones between the users and their OpenID providers. It also provides other benefits [10], like being *Resilient-to-Leaks-from-Other-Verifiers, Resilient-to-Theft* and *Requiring-Explicit-Consent*. However, it is not *Resilient-to-Internal-Observation* because malware can steal the credentials or cookies and not *Resilient-to-Phishing* as it uses re-direction in the process which could be spoofed by a phishing attack. Also, as it is based on a single identity provider, it does not meet the guidelines for the *Unlinkable* or *No-Trusted-Third-Party* criteria.

KinderSurf has the advantage of parental authorization which acts as a second factor authentication; however, the parent may not actually know for sure that it is the child logging in rather than an imposter. KinderSurf rates similarly to OpenID in terms of security benefits.

By providing these usability, deployability and security benefits, OpenID and likewise KinderSurf are a reasonable alternative to text passwords, particularly with low-risk accounts that children would have.

6.2.3 Recommendations

Based on our work and the results of this research, we make the following recommendations relating to user authentication for children.

- Systems should have configurable parental controls: Most parents from both studies wanted to keep the parental control features. These help set clear boundaries for children and transfers responsibility to the parents. It also helps parents be aware of their child's online activities.

- The authentication mechanism should be flexible: We recommend the authentication mechanism be flexible enough to incorporate various family dynamics. For example, a single parent did not want to share their credentials with the other parent while others wanted to allow other family members to also have consent authority. Some parent wanted the ability to have one-time exceptions to the rules. All of these highlight the need to accommodate a range of family situations.

- The system should encourage a proper mental model: As discussed earlier, initially parents lacked an OpenID mental model, and this affected their ability to complete tasks and their opinion of the system. Any deployed child authentication system needs to help users develop an appropriate mental model, particularly because this impacts the security and privacy of children. We do not want to accidentally put them at risk from errors caused by inaccurate mental models.

- The system should offer password choices: We recommend to provide a combination of password types to appeal to a wider audience. The child password is optional in our system. However, we received varied feedback about what type of password it should be. In the end, we selected a PIN+graphical password since our early feedback was split between PIN and graphical passwords. Participants in the second study were happy with the choice and used whichever memory cue was most useful for them.

6.3 Limitations

The main limitation in our studies relate to ecological validity due to prototype limitations and the lab settings.

Prototype Limitations: The prototype implementation had limitations that affected usability. As mentioned earlier, the rules screen had complex interaction and some functionality was implemented differently depending on screen. For example, the delete feature could usually be used by clicking on an explicit icon, but on one screen, it needed to be activated with a long press. These inconsistencies impacted user experience. Furthermore, the prototypes were not fully integrated or functional. Users had to use pre-defined accounts and a fake website. They also had to switch between prototypes to test the different functionality.

Lab Setting: We conducted our studies in a controlled and isolated environment and attempted to mimic real-life usage scenarios. However, parents and children were co-located and had limited time to interact with the software. In a real-life setting, participants would have more time to familiarize themselves with the software. Also their mental models and perception of the system may differ, when using the software in day-to-day life compared to the 60 minute session. Furthermore, participants paid full attention to the tasks because they were being observed by the experimenter, but in a more realistic setting, they may be distracted and not fully concentrate on the authentication tasks.

6.4 Future Work

We will continue to iteratively design and implement KinderSurf with Bluink, taking user feedback and preferences into consideration. We will reduce complex interactions and make the interface more intuitive. For example, we will make the rules page use sliders, and make the labels interactive. A more ecologically valid user study will be carried out to evaluate and refine the functional app. We will devise a wider range of relying party websites and have families use these in their natural setting over a few weeks to assess how well the system works in real life.

6.5 Conclusion

We aimed to develop an authentication mechanism for children. We iteratively designed, prototyped and tested a parent-child password manager that minimizes the password burden and provides parents with various monitoring controls. The user studies revealed areas for improvement but overall both parents and children liked the idea of using parental consent to log in. The parents preferred to create rules over receiving individual consent notifications. Parents noted that before they saw it, they did not even realize they needed it but now want such a tool for their family. We hope to develop a fully functional KinderSurf app that addresses the issues of child authentication.

Reflecting on our research we note several lessons that are generalizable to the larger area of usable security for children. We found that inaccurate mental models can significantly hinder users' willingness to adopt a system and their level of trust towards the security mechanism. Reflecting on our methodology we observed that parent-child pairs were much more engaged while interacting directly with the prototype as opposed to during the interview segments. We encourage researchers to offer even low-fidelity prototypes as a cue to facilitate discussion or feedback. We also noticed that many families were more comfortable participating in the session together. While ethically allowing families to stay together is appropriate, we recognized that this may influence research results. We recommend that researchers consider this dynamic when structuring their study.

Bibliography

[1] [Online] 1password.com. 1password. `https://1password.com/`, accessed: 2016-6-9.

[2] Abs.gov.au. Australian bureau. household use of information technology 2014-2015, [online]. `http://www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0`, accessed: 2016-6-9.

[3] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[4] Jonathan Arnowitz, Michael Arent, and Nevin Berger. *Effective prototyping for software makers*. Elsevier, 2010.

[5] Deepthi Bala. Biometrics and Information Security. In *Proceedings of the 5th annual conference on information security curriculum development*, pages 64–66. ACM, 2008.

[6] Carol Margaret Barron. 'I had no credit to ring you back': Children's strategies of negotiation and resistance to parental surveillance via mobile phones. *Surveillance & Society*, 12(3):401, 2014.

[7] Miki Baumgarten. Kids and the Internet: A developmental summary. *Computers in Entertainment (CIE)*, 1(1):2, 2003.

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

[9] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of Web authentication schemes. Technical Report UCAM-CL-TR-817, University of Cambridge, Computer Laboratory, 2012.

[10] Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*, pages 553–567. IEEE, 2012.

[11] S Brands. The problem(s) with OpenID. *The Identity Corner*, 2007.

[12] Amy Bruckman, Alisa Bandlow, and Andrea Forte. *HCI for Kids*, chapter 40, pages 739–809. CRC press, 2002.

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

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

[15] Sonia Chiasson. *Usable authentication and click-based graphical passwords*. PhD thesis, Carleton University Ottawa, 2008.

[16] Sonia Chiasson, Paul C van Oorschot, and Robert Biddle. A Usability Study and Critique of Two Password Managers. In *Usenix Security*, volume 6, 2006.

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

[18] Federal Trade Commission et al. Children's online privacy protection act of 1998. *Online at: http://www.cdt.org/legislation/105th/privacy/coppa.html*, 1998.

[19] [Online] Common Sense Media. Zero to eight: Children's media use in America 2013. https://www.commonsensemedia.org/research/zero-to-eight-childrens-media-use-in-america-2013, accessed: 2016-6-9.

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

[21] [Online] Dashlane.com. Dashlane password manager. `https://www.dashlane.com/passwordmanager`, accessed: 2016-6-9.

[22] Jan De Clercq. Single sign-on architectures. In *Infrastructure Security*, pages 40–58. Springer, 2002.

[23] Dorothy E Denning and Giovanni Maria Sacco. Timestamps in key distribution protocols. *Communications of the ACM*, 24(8):533–536, 1981.

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

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

[26] Arthur Evans Jr, William Kantrowitz, and Edwin Weiss. A user authentication scheme not requiring secrecy in the computer. *Communications of the ACM*, 17(8):437–442, 1974.

[27] Gunter Fahrnberger, Deveeshree Nayak, Venkata Swamy Martha, and Srini Ramaswamy. Safechat: A tool to shield children's communication from explicit messages. In *Innovations for Community Services (I4CS), 2014 14th International Conference on*, pages 80–86. IEEE, 2014.

[28] Dinei Florencio and Cormac Herley. A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web*, pages 657–666. ACM, 2007.

[29] Simson Garfinkel and Heather Richter Lipford. Usable security: History, themes, and challenges. *Synthesis Lectures on Information Security, Privacy, and Trust*, 5(2):1–124, 2014.

[30] [Online] Angela Gerber. How Young is Too Young? Introducing young children to information technology. `http://webspace.ship.edu/ejournal/contents/fall09/fall09final/how%20young%20is%20too%20young.pdf`, accessed: 2016-6-9.

[31] J Alex Halderman, Brent Waters, and Edward W Felten. A convenient method for securely managing passwords. In *Proceedings of the 14th international conference on World Wide Web*, pages 471–479. ACM, 2005.

[32] Ben Halpert. Preschool information assurance curriculum development. In *2010 Information Security Curriculum Development Conference*, pages 27–28. ACM, 2010.

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

[34] Dick Hardt. The OAuth 2.0 authorization framework. *ietf.org*, 2012.

[35] Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 New Security Paradigms Workshop*, pages 133–144. ACM, 2009.

[36] Cormac Herley and Paul Van Oorschot. A research agenda acknowledging the persistence of passwords. *Security & Privacy, IEEE*, 10(1):28–36, 2012.

[37] Ahsan Imran. A comparison of password authentication between children and adults. Master's thesis, Carleton University Ottawa, 2015.

[38] [Online] Keepass.info. KeePass password safe. `http://keepass.info`, accessed: 2016-6-9.

[39] Richard Kissel. Glossary of key information security terms. *NIST Interagency Reports NIST IR*, 7298(3), 2013.

[40] Daniel V Klein. Foiling the cracker: A survey of, and improvements to, password security. In *Proceedings of the 2nd USENIX Security Workshop*, pages 5–14, 1990.

[41] John Kohl and Clifford Neuman. The Kerberos network authentication service (v5). Technical report, 1993.

[42] M Kotadia. Gates predicts death of the password. *CNET News. com*, 2004.

[43] Leslie Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24(11):770–772, 1981.

[44] [Online] Lastpass.com. Lastpass. `https://www.lastpass.com`, accessed: 2016-6-9.

[45] Ben Laurie. OpenID: Phishing heaven. *January*, 19:187, 2007.

[46] Sonia Livingstone and Leslie Haddon. Risky experiences for children online: Charting European research on children and the internet. *Children & Society*, 22(4):314–323, 2008.

[47] Bluink Ltd. KinderSurf App Design Documents. `http://www.bluink.ca`, accessed: 2016.

[48] P Madsen. Liberty alliance project white paper: Liberty id-wsf people service-federated social identity. *Liberty Federated Social Identity*, 2005.

[49] Daniel McCarney, David Barrera, Jeremy Clark, Sonia Chiasson, and Paul C van Oorschot. Tapas: design, implementation, and usability evaluation of a password manager. In *Proceedings of the 28th Annual Computer Security Applications Conference*, pages 89–98. ACM, 2012.

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

[51] [Online] Chris Messina. OpenID phishing brainstorm. `http://wiki.openid.net/w/page/12995216/OpenID_Phishing_Brainstorm`, 2009, accessed: 2016-6-9.

[52] Robert Morris and Ken Thompson. Password security: A case history. *Communications of the ACM*, 22(11):594–597, 1979.

[53] [Online] Mozilla ver. 10.0.2. Mozilla firefox. `https://www.mozilla.org`, accessed: 2016-6-9.

[54] Roger M Needham and Michael D Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12):993–999, 1978.

[55] Donald A Norman. Some observations on mental models. *Mental models*, 7(112):7–14, 1983.

[56] [Online] Oauth.net. OAuth. `http://oauth.net`, accessed: 2016-6-9.

[57] Lawrence O'Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12):2021–2040, 2003.

[58] [Online] Openidexplained.com. Benefits of OpenID. http://openid.net/get-an-openid/individuals/.

[59] [Online] Openidexplained.com. OpenID explained. `openidexplained.com/get`, accessed: 2016-7-26.

[60] [Online] openid.net. OpenID Connect. `http://openid.net/connect/faq`, accessed: 2016-7-26.

[61] Andreas Pashalidis and Chris J Mitchell. A taxonomy of single sign-on systems. In *Australasian Conference on Information Security and Privacy*, pages 249–264. Springer, 2003.

[62] Janet C Read and Russell Beale. Under my pillow: designing security for children's special things. In *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology*, pages 288–292. British Computer Society, 2009.

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

[64] David Recordon and Drummond Reed. OpenID 2.0: a platform for user-centric identity management. In *Proceedings of the second ACM workshop on Digital identity management*, pages 11–16. ACM, 2006.

[65] Karen Renaud. Evaluating authentication mechanisms. *Security and Usability: Designing Secure Systems That People Can Use*, pages 103–128, 2005.

[66] [Online] roboform.com. Roboform password manager. `http://www.roboform.com/`, accessed: 2016-6-9.

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

[68] Blake Ross, Collin Jackson, Nick Miyake, Dan Boneh, and John C Mitchell. Stronger password authentication using browser extensions. In *Usenix Security*, pages 17–32. Baltimore, MD, USA, 2005.

[69] Natsuhiko Sakimura, J Bradley, M Jones, B de Medeiros, and C Mortimore. OpenID connect core 1.0. *The OpenID Foundation*, page S3, 2014.

[70] Jerome H Saltzer and Michael D Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9):1278–1308, 1975.

[71] Martina Angela Sasse. Usability and trust in information systems. *Edward Elgar*, 2005.

[72] Martina Angela Sasse, Sacha Brostoff, and Dirk Weirich. Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security. *BT technology journal*, 19(3):122–131, 2001.

[73] Frank Stajano. Pico: No more passwords! In *Security Protocols XIX*, pages 49–81. Springer, 2011.

[74] Frank Stajano, Graeme Jenkinson, Jeunese Payne, Max Spencer, Quentin Stafford-Fraser, and Chris Warrington. Bootstrapping adoption of the pico password replacement system. In *Security Protocols XXII*, pages 172–186. Springer, 2014.

[75] Frank Stajano, Max Spencer, Graeme Jenkinson, and Quentin Stafford-Fraser. Password-manager friendly (pmf): Semantic annotations to improve the effectiveness of password managers. In *Technology and Practice of Passwords*, pages 61–73. Springer, 2015.

[76] V Steeves. Life online: Young canadians in a wired world, phase III. *Ottawa: MediaSmarts*, 2014.

[77] Valerie Steeves. Young canadians in a wired world, phase III: Talking to youth and parents about life online. `http://mediasmarts.ca/research-policy`, accessed: 2016-6-9.

[78] Elizabeth Stobert and Robert Biddle. The password life cycle: user behaviour in managing passwords. In *Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 243–255, 2014.

[79] San-Tsai Sun, Yazan Boshmaf, Kirstie Hawkey, and Konstantin Beznosov. A billion keys, but few locks: the crisis of web single sign-on. In *Proceedings of the 2010 workshop on New security paradigms*, pages 61–72. ACM, 2010.

[80] 2015 Technical report, Office for National Statistics. Internet access households and individuals 2015, [online]. `http://webarchive.nationalarchives.gov.uk/20160105160709/http://www.ons.gov.uk/ons/dcp171778_412758.pdf`, accessed: 2016-6-9.

[81] [Online] Techopedia. Password manager. `https://www.techopedia.com/definition/31435/password-manager`, accessed: 2016-6-9.

[82] Daniel Terdniman. Google security exec: 'passwords are dead'. *CNET News.com*, 2013.

[83] [Online Tetraph.com. covert redirect vulnerability related to OAuth 2.0 and OpenID. `http://www.tetraph.com/blog/covert-redirect/covert-redirect-vulnerability-related-to-oauth-2-0-and-openid/`, accessed: 2016-6-26.

[84] [Online] Tetraph.com. OAuth 2.0 and OpenID covert redirect vulnerability 2016. `http://tetraph.com/covert_redirect/oauth2_openid_covert_redirect.html`, accessed: 2016-6-26.

[85] [Online] Klosowski Thorin. Lifehacker faceoff: the best password managers, compared. `http://lifehacker.com/lifehacker-faceoff-the-best-password-managers-compare-1682443320`, accessed: 2016-7-26.

[86] Francis Kapo Tse, Zahra Langford, Jennifer Watts-Englert, Catherine McCorkindale, David Russell Vandervort, and Mary Ann Sprague. Alternate game-like multi-level authentication, 2015. US Patent 9,122,850.

[87] Eugene Tsyrklevich and Vlad Tsyrklevich. Single sign-on for the internet: a security story. *July and August*, 340, 2007.

[88] Manuel Uruena and Christian Busquiel. Analysis of a privacy vulnerability in the OpenID authentication protocol. *IEEE Multimedia Communications, Services and Security*, 2010.

[89] Bart Van Delft and Martijn Oostdijk. A security analysis of OpenID. In *IFIP Working Conference on Policies and Research in Identity Management*, pages 73–84. Springer, 2010.

[90] Riley Walters. Cyber attacks on US companies in 2014. *Heritage Foundation Issue Brief*, (4289), 2014.

[91] Rui Wang, Shuo Chen, and XiaoFeng Wang. Signing me onto your accounts through facebook and google: A traffic-guided security study of commercially deployed single-sign-on web services. In *2012 IEEE Symposium on Security and Privacy*, pages 365–379. IEEE, 2012.

[92] Dirk Weirich and Martina Angela Sasse. Pretty good persuasion: a first step towards effective password security in the real world. In *Proceedings of the 2001 workshop on New security paradigms*, pages 137–143. ACM, 2001.

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

[94] Maurice Vincent Wilkes. *Time sharing computer systems*. Elsevier Science Inc., 1975.

[95] [Online] Victoria Woollaston. Kids ARE growing up faster today – and it's all down to technology: Facebook and mobile phones causing children to mature more quickly, poll reveals. `http://www.dailymail.co.uk/sciencetech/article-2834559/`, accessed 2016-6-9.

[96] Jeff Yan, Alan Blackwell, Ross Anderson, and Alasdair Grant. The memorability and security of passwords. *Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, eds*, 7:129–142, 2005.

[97] Bian Yang, Huiguang Chu, Guoqiang Li, Slobodan Petrovic, and Christoph Busch. Cloud password manager using privacy-preserved biometrics. In *Cloud Engineering (IC2E), 2014 IEEE International Conference on*, pages 505–509. IEEE, 2014.

Appendix A

Child Questionnaire Study-1

A.1 Pre-Questionnaire

Do you know what a password is?
Do you have any passwords?
Which devices do you use?
If you have a device password, what type do you use?
Do you create them or mom/dad?
What are your favorite websites? Do you use youtube? What games do you play?
Do you have more than one password?
What happens if you forget the password of your phone/ipad/computer/laptop?
Do you share your passwords with your parents?
Would you share your password when your friends ask you for it when they visit your place?
How about, if your teacher at school asks for your password?
Would your share your password with a stranger/ any person you don't know?

A.2 During Tasks

If you were given an option to set password from these four types, which one would it be? And why?
Which one of the four password types, did you not like and why so?

A.3 Post-Questionnaire

Okay so how was it? Did you like the idea of using one password to enter in all accounts?
And how you think we could make it better.

Is there something you liked very much?

Is there something you did not like at all?

Is there anything that you want to say?

Appendix B

Parent Questionnaire Study-1

B.1 Demographics

How old is your child (participant)? gender?
What grade in school?
How many siblings?
Parent gender?

B.2 Pre-Questionnaire

How many accounts do they have?
What device do they use to browse online?
What kind of websites does your child visit?
How frequently?
Can you tell me what steps you take to make sure they are safe online?
What kind of parental controls, if any, do you use?
How many passwords does your child have?
Do you share them? How do you teach them not to share it with anyone else?
Who is responsible for creating accounts/passwords and how does this normally happen?
Can you give an example of when you had a problem with your childs account/password?
How do they remember passwords? What if they forget?
Do you know what a password manager is? If yes, do you use any for your children?

B.3 During Tasks

If you were given an option to set password from these four types, which one would it be? And why?
Which one of the four password types, did you not like and why so?
Do you prefer to create your own password or use generate password?

B.4 Post-Questionnaire

Would a parent/child password manager be helpful in your family? How would you like it to work?
What did you feel was missing in the prototype?
How can we make it better?
Did you find anything that was there in the prototype, but you would not use it.
Did you like the prototype?
What did you like in the prototype?
Would you use it?
Did you find the names confusing? (Parental control / Password manager) If yes, can you suggest names?
What would make things easier?
Anything else you would like to say/mention?

Appendix C

Child Questionnaire Study-2

C.1 Pre-Questionnaire

Do you know what a password is? Yes/No
Please describe it.
Do you have any passwords? Yes / No
Name the websites you log in to. Do you have a Facebook or Gmail account? School email? Games? Any other?
Which device you use the most? (Computer / Laptop / Mobile device / Tablet / Other)
When was the last time you logged in?
What happens when you log in?
Do you need permission to log in? Who gives you?
What if a parent says dad/mom, do you ask mom/dad?
What do mom and dad ask you before you are allowed to log in?
Do you and your sibling access accounts / share password? When? How?
Do you and your sibling have different rules. YES/NO?
If yes, which rules are different?
Who creates your passwords? (You / Mom / Dad / Sibling / Others)

C.2 During Tasks

Do you like the password type (PIN + graphical)?
Would you send a notification to parents for logging in?
Do you think it is a good idea that if mom and dad allow you to a website, you can log in to anywhere with just 1 or no password?

Would you prefer to have 1 password or none?

Will you send a message? Would you prefer to type a message or select emojis.

C.3 Post-Questionnaire

Did you like the idea of using parental consent to enter in all accounts?

Would you prefer this over current authentication system?

Any suggestions? how you think we could make it better.

Is there something you else you want to say?

Appendix D

Parent Questionnaire Study-2

D.1 Demographics

How old is your child (participant)? gender?
What grade in school?
Parent age or age range? gender?
What is your occupation?
How did you learn about computers and online security.

D.2 Pre-Questionnaire

Which device does your child use the most? (Computer / Laptop / Mobile device / Tablet / Others)
Do you talk to your children regarding how to be safe online?
Do you know when your child is online?
Do they take your permission every time they are online?
Are there any rules set?
Different rules for siblings if any?
How does your child log in to a website? What does he usually say?
How do you decide to allow our child or not?
Do you ask the kids to do anything before permitting? What?
Have siblings logged in from each others accounts. Do they share passwords?
Have you ever seen a Single-Sign on sign-in? Like Sign in with Facebook or Sign in with Gmail? Used Single-Sign on?

D.3 During Tasks

Do you like the password type (PIN + graphical)?
Would you use a password or none for children?
How like are you to reply with message? Would you prefer one time message or conversation like messages?)
Would you prefer children to ask permission each time or set up rules?
You would like to view history for successful logins only or failed as well?
Would you use it over multiple devices/caregivers?

D.4 Post-Questionnaire

How likely are you to use an app such as this for your child to log in? (10-Point Likert-Scale from Not At All to Very Likely)
If using this app, how likely are you to set up auto-accept or auto-deny rules for individual websites? (10-Point Likert-Scale from Not At All to Very Likely)
If using this app, how likely are you to have every login request be dealt with individually (e.g., no auto-allow or auto-deny rules)? (10-Point Likert-Scale from Not At All to Very Likely)
How much would you pay for this service initially? ($0, Up to $2, Up to $5, Up to $10, Up to $15, More than $15)
How much would you be willing to pay monthly for this service? ($0, Up to $2, Up to $5, Up to $10, Up to $15, More than $15)
On which types of devices would you like to be notified on? (Android/iOS)
On how many devices would you install this app? (1, 2, 3, 4, 5, More than 5)
Who would be allowed to provide consent? (Can check multiple: Mom, Dad, Caretaker/babysitter, Older sibling, Grandparents, Others)
How many different websites does your child log in to?
For what ages of children do you think this app is appropriate? (Under 4, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, Older than 14)
Which authentication system would you prefer? Current system or Proposed app ?

Do you have any suggestions? how you think we could make it better? What have we missed?

Do you have any other feedback?