No passwords needed: The iterative design of a parent-child authentication mechanism

Kalpana Hundlani, Sonia Chiasson
Carleton University, Ottawa, Canada
KalpanaHundlani@cmail.carleton.ca,
chiasson@scs.carleton.ca

Larry Hamid
Bluink Ltd
https://bluink.ca/
lhamid@bluink.ca

ABSTRACT
Even though the vast majority of children are online, our exploration of the user authentication literature and available tools revealed few alternatives specifically for authenticating children. We create an authentication mechanism that reduces the password burden for children and adds customizable parental oversight to increase security. With Bluink, our industry partner, we iteratively designed and user tested three parent-child prototypes, with each iteration addressing issues raised in the previous iteration. Our final design is a parent-child authentication mechanism based on OpenID and FIDO U2F which allows children to log in to websites without requiring a password and enables parents using their mobile device to remotely determine whether a login request should be granted.

Author Keywords
Authentication; children; parents; mobile device; user study

ACM Classification Keywords
K.6.5 Computing Milieux: Security and Protection - Authentication

INTRODUCTION
By 2014, 99% of Canadian children aged 8-15 years were online outside of school [33] and 72% of children under 8 used mobile devices [10]; both statistics represent sharp increases in recent years. Similar statistics are available in other countries [4, 19, 22]. Although parents enable this access, they also express worry. In 2000, Canadian parents were primarily enthusiastic about the opportunities offered to children through increased connectivity, but by 2011 the sentiment had shifted to one of insecurity and fear for their children [32]. Research suggests that a third of Canadian children 8-11 *never* have an adult present when they are online [33], making it especially important that age-appropriate security mechanisms are developed. Children often have accounts to access content online [11, 33, 35], typically secured with an alphanumeric password. However, password schemes and policies have historically been designed with adults in mind, and have significant drawbacks [6] even for adults. For example, they have usability issues, primarily linked to memorability and understanding of 'good' passwords [39].

Like adults [34], children demonstrate difficulty with passwords and resort to coping strategies [3, 40]. The task may be particularly difficult for children given that they are still developing cognitive abilities [25, 30]. This suggests that alternative mechanisms are needed; however, the field of child authentication has received very little attention. There exists only sparse research on children's performance with existing mechanisms [3] and few child-friendly authentication schemes [21, 36]. Thus far, solutions have tended to focus on parental monitoring tools [7, 9, 12, 13].

We wanted to simplify child authentication while maintaining the security of the protected accounts. In particular, we wanted to remove the burden of authentication from child and use a mobile solution to give parents the authority to allow or deny a login to a particular service by the child without requiring that the parent be physically present. This research was a joint project between our academic research team and a local technology company. Through an iterative process, we designed and user-tested three different prototypes with parents and children; each prototype addressed issues raised in the previous iteration. This paper describes this design process, addresses the successes and failures of each design, details our final mobile prototype, and concludes with insight based on our experiences. Our scope was limited to children aged 7–11 years logging onto websites, but could be extended.

In our initial attempt, we explored the feasibility of a mobile parent-child password manager. The password manager achieved password reduction and included parental controls to shift the burden of managing passwords on to adults. However, we found that this was not sufficient. Our second prototype was based on OpenID [28] and the FIDO universal two-factor authentication standard(U2F) [31]. This second prototype also involved parents in the authentication decisions. Based on the feedback from the second user study, we created the third prototype and evaluated it with participants as well.

Th main contributions of this paper are: (i) Exploring the feasibility of a parent-child authentication mechanism, (ii) Designing, developing, and user testing three mobile prototypes, (iii) Presenting insight based on our experiences.

MobileHCI 2017, September 4–7, 2017, Vienna, Austria

ACM ISBN ??. . . $15.00
DOI: ??

BACKGROUND

Knowledge-based authentication, such as passwords, will likely remain the dominant method of user authentication [16] for the foreseeable future despite their many usability and security problems [15]. However, in some circumstances, it is desirable to consider alternatives. We suggest that it is unreasonable to expect children to effectively manage the complexities of passwords such as knowing how to create secure passwords, handling the memory burden associated with strong passwords, and knowing how to securely manage passwords (e.g., when and how is it safe to disclose them?).

Password Managers: One plausible alternative is a password manager that stores and organizes passwords to help achieve password reduction [15, 18]. Password managers may also offer a variety of services, such as password-strengthening and phishing protection. Most implementations require no server side changes so they can be easily integrated into current authentication schemes. They reduce login time and facilitate the use of stronger passwords. Bonneau et al.'s authentication evaluation framework [6] evaluates web authentication schemes in terms of usability, deployability and security. They find that password managers are better in terms of usability and security compared to passwords despite their potential single point of failure and need to migrate accounts, but that passwords remain more deployable. Building on these findings, we concentrate our efforts on password managers [18] and other means of reducing the password burden from users.

Most research on password managers has focused on the underlying technical details; only a few have assessed of their usability and its effects on security. For example, Chiasson et al. [8] evaluated usability of two password managers, finding that usability and trust are significant barriers to secure adoption, with several instances of users unknowingly exposing their accounts. A dual-possession password manager called TAPAS was introduced by McCarney et al. [20] where a nearby mobile device was used to securely transmit a password to a paired device/computer, eliminating the need for a master password and helping users form an accurate mental model of the system. Thus far, we have found no child-specific password managers nor evaluations of their use with children.

OpenID and Universal Authentication Framework: Other approaches to addressing the password problem are also of interest for this paper. The OpenID OAuth 2.0 framework and its implementation protocol OpenID Connect [24, 29] support decentralized user-centric authentication, enabling a user to create an account with any OpenID identity provider, such as Google, and use their OpenID credentials to login to any co-operating websites (relying party) [37]. The OpenID Connect protocol is based on JSON and RESTful HTTP API. The identity provider manages credentials and processes authentication requests for the relying parties. OpenID technology provides advantages [23] like password reduction, speedy sign up, interoperability, and user control over their online identity.

The FIDO Alliance [1] offers two specifications for authentication protocols: Passwordless (UAF) and Second Factor (U2F). FIDO's protocols rely on public key cryptography (PKI), perform key exchange, and rely on signing login challenges to verify the identity of clients. The Universal Authentication Framework (UAF) [1] provides password-less online authentication through the use of physical tokens or local authentication (such as entering a local biometric). Online services can enable use of a range of local authentication mechanisms, also removing the need for the online service to store and manage authentication credentials, and freeing users from having to remember passwords. The UAF service authenticates a device and then trusts local authorization to verify the user from that device. On the other hand, the Universal 2nd Factor (U2F) [31], offers secure second factor authentication. Users login with the first factor in the usual manner (e.g., with a PIN or password), then provide a second factor in the form of a hardware device/authenticator which stores a user's private key and can be used to respond to a login challenge. Whenever U2F is requested, the user provides the pre-registered device as proof of identity. Both OpenID Connect and the FIDO standards have enjoyed increasing support from major online service providers (e.g., Paypal, Google, Microsoft, Amazon, WordPress), and there have been some efforts at creating technologies that merge the two approaches.

Children: Research about online security for children typically emphasizes parental controls or other monitoring tools. For example, an automated tool named POCKET [7] was devised to enforce the US Children's Online Privacy Protection Act [14], while SafeChat [13] and other online messaging tools aimed at children provide encryption, offer parental monitoring, and filter abusive words. Other alternatives include hardware solutions, such as the Circle [17] device that pairs with a home router and monitors all traffic via ARP spoofing. It aids parents in managing all connected devices through setting age filters, configuring screen-time for devices and pausing internet access. The Circle Go app manages devices outside the home network via VPN. More specifically for mobile devices, the Limitly [26] app aids parents in tracking app usage and setting screen-time limits. It also blocks children from using apps that are not reviewed by their parents.

There exists sparse research on child authentication. Read and Cassidy [27] carried out user studies with children aged 6–10, looking at how children create passwords and investigating the types of passwords they used. Mendori et al [21] designed an icon-based authentication mechanism for children unfamiliar with the alphabet. Tse et al. propose an iterative authentication scheme [36] similar to a game for young children. Recently, a comparison [3] of three graphical password schemes was carried out, showing that children preferred passwords consisting of selecting cells with images of distinct objects from among decoys in a grid. Zhang-Kennedy et al. [40] explored how families managed passwords. They found that adults usually bear the burden of managing children's passwords, that children frequently forget passwords, and that families often resort to weak passwords to cope.

In this paper, we work towards finding an alternative authentication mechanism for children. Furthermore, our final solution combines OpenID Connect and U2F in a novel way that enables a parent to submit credentials through their mobile device on behalf of the child wishing to log in to a website.

To-date, these protocols have only been used in single-user scenarios rather than having one user vouch for another in the authentication process.

METHODOLOGY

We employed an iterative process where we designed a prototype, conducted a user study with parents and children to evaluate usability and collect feedback, then redesigned the prototype based on the results. In total, we designed three prototypes with increasing fidelity, and conducted three user studies. The user studies largely followed the same methodology and were used as formative evaluations to guide the design process. When available, parent-child pairs participated in more than one iteration so that we could collect comparative feedback on the progress of the prototype. The first two studies included 20 participants each (10 parents and 10 children per study), while the last study included 30 participants (15 parents and 15 children). All studies were conducted in the lab and involved the children and parents completing typical tasks with the prototypes on laptops and mobile devices, providing feedback through interviews, and completing questionnaires. The children in our studies were between 7–11 years old and attended the sessions with a parent.

All three studies were reviewed and cleared by our institution's research ethics board. Parents completed written consent forms and the children gave verbal assent; both had to independently agree to the study to participate.

In the following sections, we first describe the three prototypes, including results of the user studies as they relate to guiding the next iteration. We include more detail about the study methodology and results of the last user study which evaluated our third prototype.

PROTOTYPES

In this section, we describe the progression from our first low-fidelity prototype to our final high-fidelity iteration of the proposed authentication system.

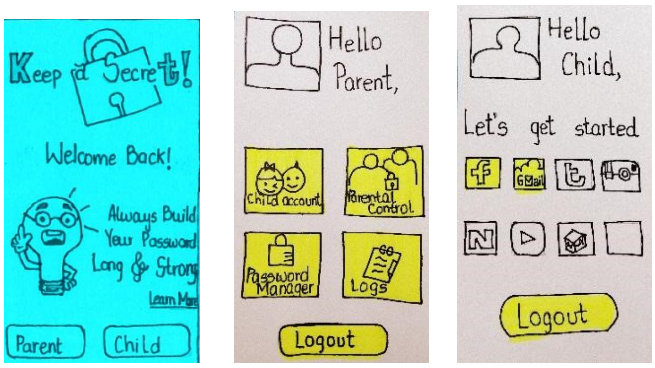
Prototype 1

After exploring existing solutions for child authentication, we proposed a parent-child password manager which would 'remember' passwords for the child and could be configured by parents. We created an interactive low fidelity mobile app prototype that would enable users to interact with the prototype and provide us feedback to redefine our design. The goal was to provide a tangible artefact for participants to consider and help articulate their requirements in relation to child authentication.

We hand-sketched 25 individual screens on paper and rendered them interactive using Prott[1]. In Prott, we linked the screens and made them responsive to click/tap and swipe gestures. Representative screens are illustrated in Figure 1.

This prototype was devised with two user groups in mind, parents and children (Figure 1a). Key features of this prototype enable parents to (i) manage accounts for multiple children, each potentially containing credentials for several websites,

[1] https://prottapp.com/



(a) Welcome screen. (b) Parent homepage with access to settings and logs. (c) Child homepage with links to permitted websites.

Figure 1: Prototype 1 sample screens

(2) set up parental controls granting a child access to permitted websites according to a predefined schedule, and (3) view a child's login history (Figure 1b). Furthermore, it provides access to all of a child's permitted websites together on one screen protected via a single master password, and thus frees them from remembering and managing passwords (Figure 1c).

From the first user study, we collected information about parent and child password habits as well as feedback on Prototype 1. Our participants reported that children access the internet through multiple devices, with tablets and laptops being most popular. Most parents reported having to deal with children forgetting passwords and locking accounts due to multiple incorrect attempts, and, as a result, resorted to coping strategies such using as weak or no passwords when possible, writing down passwords in easily visible locations within the home, and reusing passwords across accounts. No one currently used a password manager for their child. The children were shown text, graphical (selecting images from a set), and numerical (PIN) passwords; they indicated preference for graphical passwords and PINs.

As feedback on the prototype, 7 out of 10 parents said that they would use such a tool if it was available. Participants generally liked the idea but some asked for additional features, namely for email/phone notifications of the child's activities, while others asked for fewer settings. Highlighting the differences between families, a few parents requested that the tool provide total surveillance on their child's activities, while a few others disliked the idea of a parent-controlled password manager because 'they trusted their child'.

Prototype 2

We recognized that simply transferring the task of password management to parents was insufficient. Several parents preferred the idea of additional parental controls and mentioned many difficulties with passwords. We chose to explore a solution that would largely eliminate passwords without weakening the security of the child's online accounts.

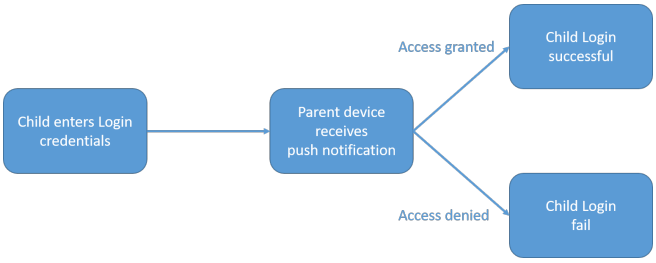


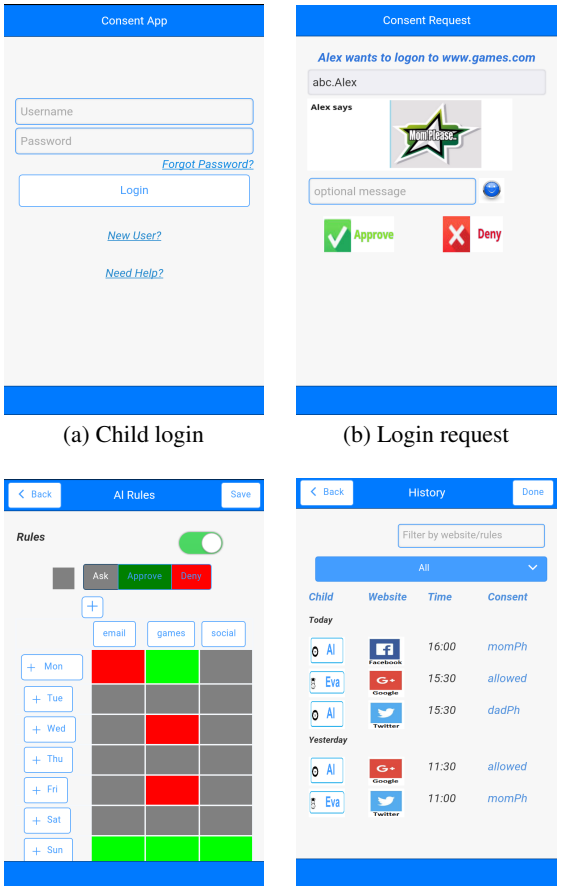
Figure 2: Prototype 2 login workflow

Our second prototype was a medium-to-high fidelity parent-child authentication mechanism based on the OpenID and U2F protocols. It enables parents to allow or deny authentication requests from their children for supported websites, and without the need for the child to enter a password. In this scheme, the child visits a supported website from any device, enters their username, and sends an authentication request to the parent device through push notifications. The parent can remotely approve or deny the request, which determines whether the child is logged in to the website. The parent can configure their app to automatically approve or deny requests for certain websites based on a pre-determined schedule. For example, a parent may decide that the child can always log in to a given game website between 3pm and 4pm on weekdays without waiting for explicit permission, or may decide that all requests be automatically denied after 9pm.

Depending on the family, some children may always be near their parents when they request access to websites, and so the parent can verify through offline channels that it really is the child attempting to log in (e.g., calling out from the next room). As an additional layer of protection, an optional master password can be set for the child. This password is presented on the website using a traditional PIN interface, except that each cell contains both an image and a digit to help with memorability. In this way, a parent has additional assurance that it really is the child requesting access in situations where offline verification is inconvenient. It also satisfies children's concern that a sibling or friend gains access to their account. The prototype also provided functionality to include an optional message/emoji with the authentication request and response for a brief online conversation between the parent and child.

We designed the UI, defined the user interaction model and workflow of the prototype. Ideally, we would have had a single prototype incorporating all of the desired functionality as per our design. However, due to our industry collaborator's time constraints and development cycle, we had two complementary prototypes, each demonstrating different features, that together covered the full range of functionalities.

Our second user study had parent-child pairs interact with the interface on mobile devices/iPads. The pairs could actually complete (and deny) the authentication process across multiple devices with a fictional website. Other parental functionality, such as creating child accounts and setting schedules for automatically accepting/denying requests, was tested through a medium-fidelity user interface.



(a) Child login (b) Login request

(c) Rule configuration (d) Login history logs

Figure 3: Prototype 2 sample screens

Participant demographics for this study were similar to the previous study. Children primarily used tablets to go online, they had passwords for a handful of accounts (although three of the youngest participants used accounts that auto-logged in so that they did not need to worry about passwords), and similar coping mechanisms were reported. Six children said that they currently need to ask permission from their parent to log in online.

The study revealed that most parent-child pairs could easily complete the login process; however, the three 7–8 year olds who usually auto-logged in had difficulty because they had never encountered a login process before. Eight of the children wanted a master password and most families wanted some form of messaging as part of the process. Parents faced some difficulty with the configuration tasks. Some issues were due to limitations of the medium-fidelity prototype, but others were with the design of the interface. For example, rules could be defined using a timetable interface, where users selected the type of rule (always-ask-for permission, automatically-approve, automatically-deny) and highlighted the days/times to which the rule was applicable. Parents were initially confused by the interface, neglecting to enable a rule once created or clicking on inactive interface elements. Apart from design

improvements, we gained knowledge of user needs and preferences to tailor the proposed solution further. Despite the initial confusion, 8 parents said they would configure rules rather than attending to every individual login request. One noteworthy feature request came from a parent who mentioned needing a 'override' option to temporarily disable rules and return to an always-ask-for-permission state for situations such as a child needing exceptional access to complete homework.

Prototype 3

We iterated our design based on participant interactions with previous prototypes and the feedback provided. From this improved design, Bluink developed a high fidelity prototype of the authentication mechanism, entitled *KinderSurf* (Figure 5). Multiple fictional websites that supported OpenID authentication were created for parent-child pairs to test the login process. *KinderSurf* is based on the OpenID Connect and U2F protocols and largely follows the same design as our second prototype.

Child interaction: A typical login interaction unfolded as follows. A child visits a compatible website, clicks the login button (Figure 4a), and enters their credentials. At minimum, the child enters their OpenID username (Figure 4b), but may also enter their master graphical/PIN password if it is enabled for the child's account. The website waits for a parent device to respond to the authentication request (Figure 4c). If access is granted, then the child logs in, otherwise an error message is displayed. Parents may also auto-allow/auto-deny requests through pre-configured rules which would respond immediately to a child's login request.

Parental controls: Besides receiving push notifications when their child requests login permission on a website, the parental mobile app enables parents to register new devices attached to their account, create and manage associated child accounts, configure access rules on a per child and per website basis (rules can also be duplicated and modified between child accounts or across websites), set an optional master password for the child, and view a child's login history.

USER STUDY 3 METHODOLOGY

We also conducted a lab-based user study for the final high fidelity *KinderSurf* prototype with 30 participants. We had 15 parents (4 males, 11 females; mean age = 40.3 years), and 15 children (9 males, 6 females; mean age = 9.2 years); 7 pairs had previously participated in studies of the earlier prototypes.

The studies followed the same general process for each participant: (i) pre-test interview relating to current online and password practices, (ii) prototype testing with specific tasks, (iii) post-test interview pertaining to their experience with the prototype, preferences and overall feedback. Interviews were audio-recorded, and the researcher took notes during the session about task completion, challenges observed, and other noteworthy events. Sessions lasted approximately 60 minutes in total per family. We completed the sections involving the children first, then gave them activities to entertain them (e.g., small crafts, colouring) while we worked with the parents.

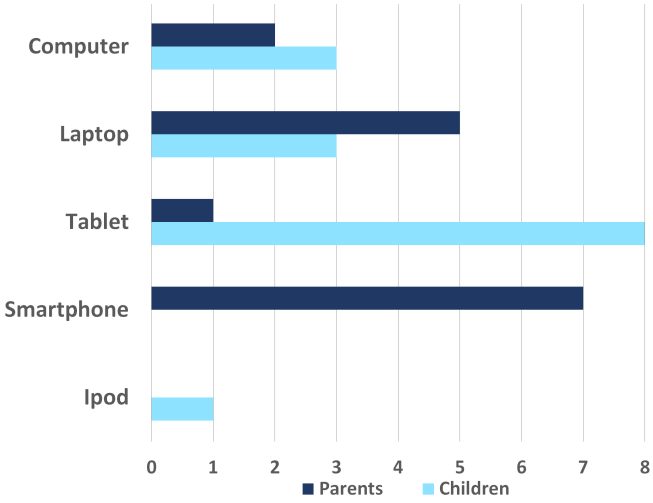


Figure 6: Most frequently used device by parents and children. Each participant could select only one option.

The children's tasks also involved the experimenter interacted as the parents. The children requested login and were approved by the parent/experimenter for the first website, logged out, and then attempted to login but the parent/experimenter denied the request. Children were then interviewed about their opinion of the system and what they would do under various circumstances, such as when a parent denies their request.

The parents subsequently interacted with the other features of the parental app, completing tasks relating to registering new devices, adding and editing child accounts, adding and editing rules, temporarily overriding rules, viewing their child's login history, and seeing what happens when multiple parent devices are registered and child login requests arrive. Parents were then interviewed about their impressions and feedback.

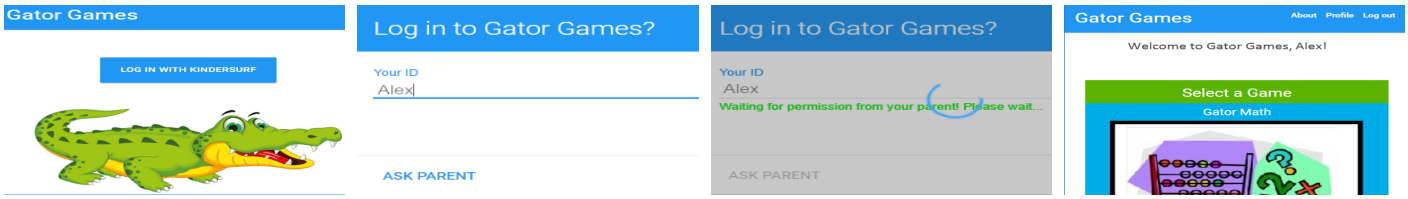
USER STUDY 3 RESULTS

We first summarize responses to the pre-interviews, followed by results from using the prototype, and feedback from the post-interview and questionnaire.

Online behaviours

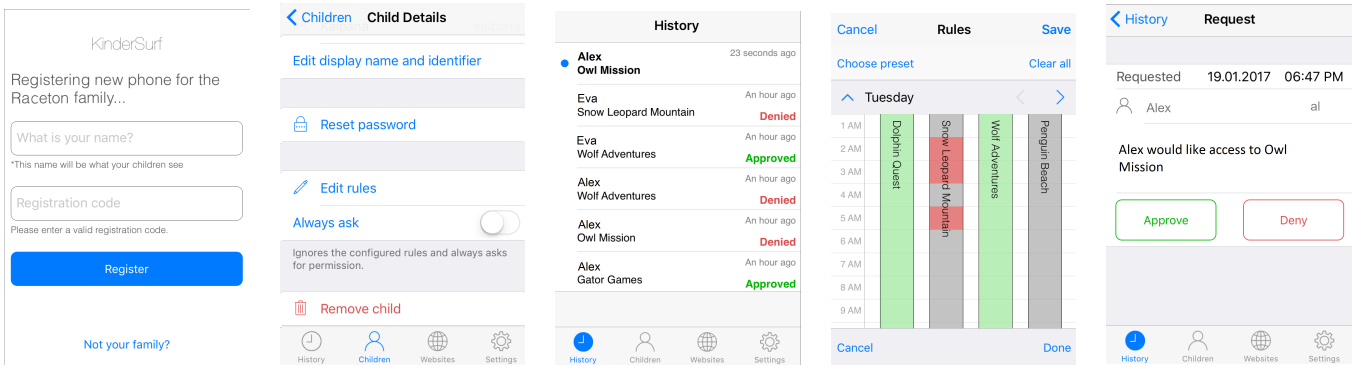
Children had between 1 and 10 accounts, with a mean of 3 accounts per child. We asked both parents and children whether the child needed permission before going online; Figure 7 highlights the difference in opinion between the two groups, with more parents believing that children require permission. We asked the children whether their parents knew when they were online; 8 said yes, 2 said their parents did not know, and the remaining 3 said maybe.

Approximately three-quarters of participants (73% of children, 80% of parents) said it was acceptable for children to share passwords within the family. We asked children how they chose a password and the most common responses were to use 'the usual one' or to reuse an existing password. We asked



(a) Click on Login with *KinderSurf* (b) Enter credentials (c) Wait for parental consent (d) Access granted

Figure 4: Prototype 3: *KinderSurf* child login session



(a) Register Device (b) Child Details (c) History (d) Rules (e) Login Request

Figure 5: Prototype 3: *KinderSurf* sample parental app screens

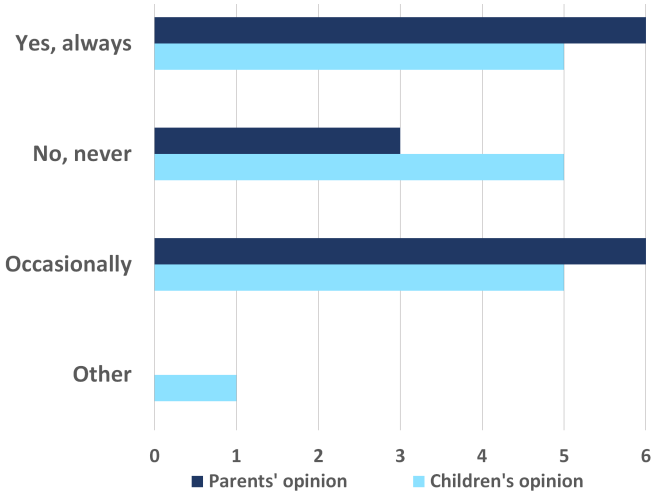


Figure 7: Responses for *{do you} / {does your child} need permission to go online?*

children whether they would like to have only one password for all accounts. Many mentioned that it would be convenient to remember only one password, but recognized the danger if someone learned the password.

As seen in Figure 6, mobile devices are very popular among our participants. More than half of children primarily used tablets to go online, while others used computers and laptops. Half of parents reported that their smartphone was their primary device, followed by laptops and computers.

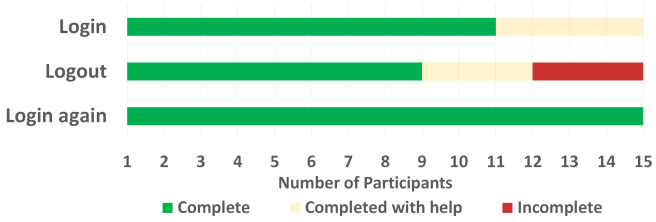
Children Tasks

As shown in Figure 8a, most children were able to complete all of the tasks, although some needed help initially. For the first task, 11 children were able to request login without help, while remaining completed with some help. However, when asked to log in to a second website, everyone did so without assistance. Some children needed assistance to locate the logout button (which may be more a reflection of our test website's design than the children's inability to logout). The three children who 'failed' the task actually closed the browser window rather than press the logout button.

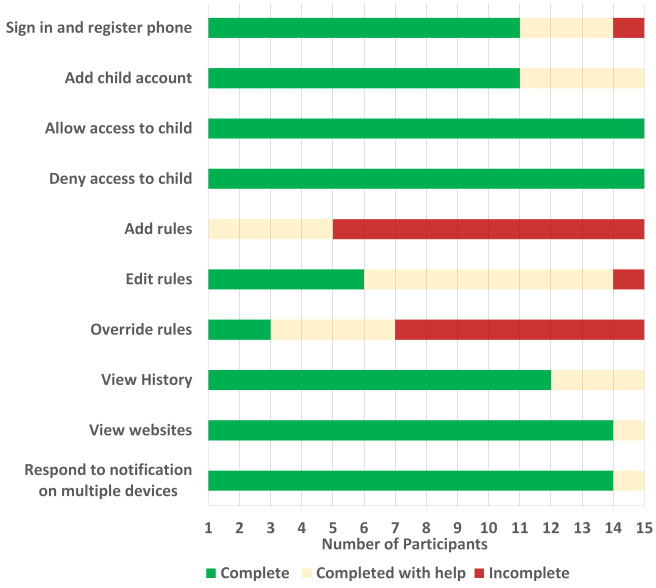
With the first login, the parent/experimenter approved the authentication request so the child logged in successfully. For the second authentication request, the parent/experimenter denied access. At this point, we asked the children what would they do if they were denied access. Most children said they would try a different website. Some added that they would ask their parent in-person or via text/email why they were denied. One child said she would keep sending authentication requests until her parent approves the login. Clearly the system should monitor for such inappropriate repeat requests and implement a configurable delay or lock-out function.

Parent Tasks

Figure 8b summarizes the tasks completed by the parents. The parental tasks were more numerous and more complex since they required activities such as configuration of parent devices,



(a) Children



(b) Parents

Figure 8: Task completion summary

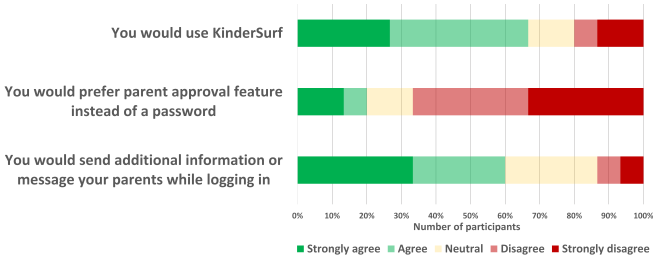
child accounts, and access rules. Parents were generally able to complete the assigned tasks; some required minor guidance from the experimenter, but then could accomplish the task.

The Rules interface was most problematic because the tasks were more complex, but also because the interface had some inconsistencies that led to usability issues. In particular, parents initially had difficulty locating and using the Rules page (under the Child tab); parents were confused because the page required both horizontal and vertical scrolling but these used different gestures, and they expected some of the labels to act as buttons. Once they had a chance to explore the interface and get some clarification, all but one parent was able to complete the second rules task. Another task where parents had difficulty was to find the exception button to override the rules. The option was located on the Child tab, but parents expected it on the Rules page.

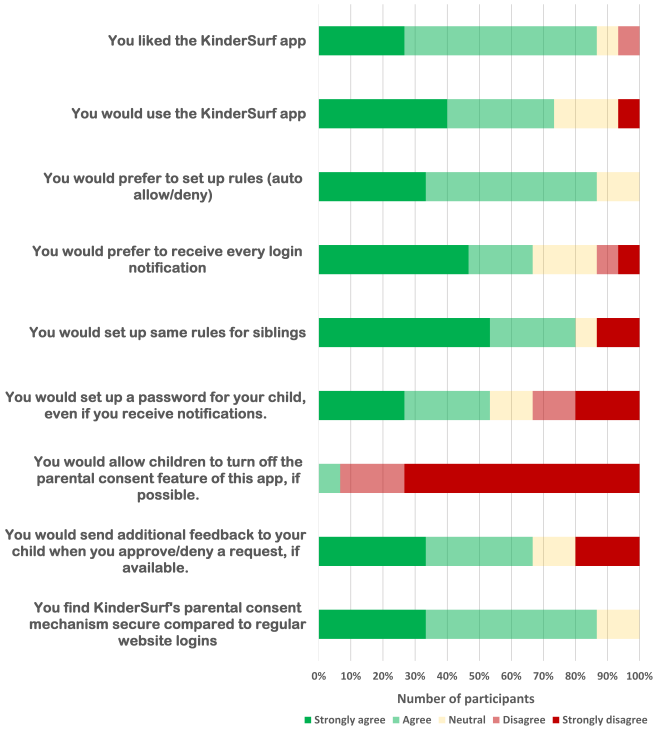
Post-questionnaire

After interacting with the system, participants answered questions relating to their experience with the prototype.

Children: As shown in the Figure 9a, 10 children agreed to use *KinderSurf* after having tried it. We asked children if they would prefer to log in the 'usual' way (i.e., with a password) or with *KinderSurf*. Children said they preferred passwords



(a) Children



(b) Parents

Figure 9: Post-questionnaire responses

because they did not want to wait for their parents to respond to login requests. We note that this would largely be mitigated if parents set up auto-accept rules for known websites and an agreed upon schedule. Twelve children would still want some form of password to login even with the parental oversight because they felt it would be safer.

In contrast with parents who feel that parental control is necessary, the children were not as enthusiastic. If given the option, most children would prefer that their parent is simply notified that a login occurred, rather than having the parent give explicit permission. Lastly, eight children would turn off the parental control feature if it was possible.

Parents: Parent responses to Likert scale questions are available in Figure 9b. Most parents liked the idea of *KinderSurf* and would use it if available. Parents also agreed that they would use functionality like creating 'auto allow/deny rules'. Despite having a complex interface, all parents appreciated the rules feature. Furthermore, when parents were asked if they

would add the optional child password, we received mixed responses. The most common reason given for not adding a password was that ultimately it would be the parents who would have to remember it. Not surprisingly, most would not want their child to have the ability to disable the parental consent feature. Parents also said they would send additional feedback to their children through the app. Finally, parents viewed *KinderSurf* as more secure than regular websites.

Suggestions: We solicited suggestions from both groups on improving *KinderSurf* and how to make it more intuitive.

Children requested more privacy options on their end, including the ability to turn off parental consent. Children understood that their parent would be a better judge of whether the website they are visiting is safe. However, they did not like the idea of waiting for the parent to provide a response.

Parents generally liked *KinderSurf*. They requested additional features, turning it into a more full-fledged parental monitoring system. They requested the ability to remotely log out their child from a current website, to set daily screen-time limits, to monitor the total time spent on websites, and to configure device priority when more than one parental device is registered. Moreover, they found the Rules screen a little confusing on their first encounter and suggested having some sort of demo help on first use.

KINDERSURF SYSTEM ARCHITECTURE

In designing *KinderSurf*, we had several technical requirements. The first was to find an architecture that would work across all platforms (e.g., web, native apps, PCs, mobile devices). The second requirement was to select an architecture that would be easily adoptable by children and parents, but also easily adoptable by the industry.

This drove us to leverage the OpenID Connect [24] and FIDO U2F technology [31], as shown in Figure 10. It is unique from other efforts at merging the two technologies because two different users take part in the authentication process. It is initiated by the child, who triggers the OpenID (first factor) authentication, which in turn triggers the U2F protocol (second factor) and requests a response to the login challenge by the parent's remote mobile device. Both the child's OpenID account (and optional password) and the pairing of the parent device to the account occur a priori during a registration phase. The scheme uses the U2F network registration and authentication protocol, but does not require a separate hardware authenticator (such as a USB device).

During login, a child initiates a login request by entering their OpenID (unique id) and optional password, which is used by OpenID provider to look up the authorizing parent userid and device. Usually, the OpenID provider authenticates the users by their credentials alone. However with *KinderSurf*, if this initial authentication is successful, it further queries the parent's device. FIDO U2F uses the parent's device as the second authentication factor and verifies the authorization identity. The parent device receives a push notification that provides the child id and the website to be accessed. The U2F challenge occurs in the background. The parent's decision to allow or deny login is conveyed to the OpenID Connect

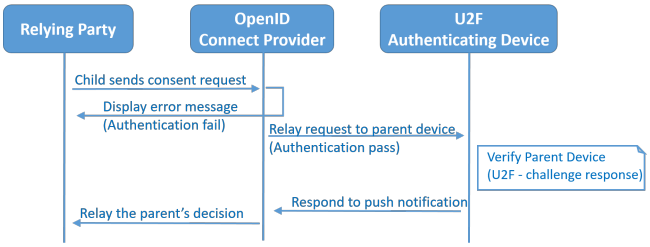


Figure 10: *KinderSurf*'s system architecture

provider, that in turn either authorizes the request or denies access to the website on the child's device. Given that parents authenticate the child and each request, the OpenID passwords are optional for children.

DISCUSSION

Apart from design improvements and suggestions for additional features, the user studies provided additional insight.

Importance of Iterative design and prototyping: The design of our prototype evolved over three complete iterations. Each iteration helped us recognize and correct flaws, gather additional requirements, and make the system more usable. We found that participants were engaged and able to envision themselves using the product when they could interact with a prototype, enabling them to consider additional features and consider what would make the most sense for their family. In particular, we found that children were more engaged when interacting with the prototype versus when being interviewed. While carrying out a task, the children 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.

Our experience supports the benefits of early and frequent prototyping, particularly when the tool being designed is addressing a problem from a novel perspective. Our parents did not initially understand the benefit of *KinderSurf*, but once they had a chance to experience it and have a say in shaping its functionality, many recognized its value and wanted to know when it would be ready for the market.

Furthermore, the progression from lower to higher fidelity prototypes demonstrated a shift in participant feedback. Parents were much more willing to offer extensive feedback on the low-fidelity prototypes and offer suggestions for new features; it was evident that the parents saw it as an idea on paper to which they could contribute and not an app already built. The children, however, offered more thorough comments and suggestions with the higher-fidelity prototypes. It seems that the children had more difficulty envisioning use of the tool when it was still in low-fidelity stages but then had stronger opinions once they could actually try it out. With the low-fidelity prototypes, the children focused on (trivial) missing functionality. For example, if one website icon was enabled for clicking in the prototype as an example, the children told us that they wanted to click on the other websites.

User Studies with Children: Ideally, the child and parent portions of our user testing session would have been 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 the children were comfortable. In our methodology, parents remained nearby but were encouraged to sit apart from their child. However, there were instances when the 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 for advice. We further found that children sometimes changed their answers depending on whether they thought their parent was listening (in these instances, we included the 'alone' answer if we were tabulating responses). For example, children were more likely to admit that they would try to disable the parental controls when their parent was not listening. Thus, to the degree that it is feasible, we recommend conducting the interactive prototype tasks together but separating the parent and child for interviews and feedback.

When working with children, we found that interaction with the prototype engaged them more than the pre and post interviews. This is likely because the prototypes provided more context versus having to imagine a hypothetical situation or remember interaction that had occurred previously. Furthermore, we recommend that sessions with children be short and have very specific tasks. Although fairly obvious, it is worth re-iterating the importance of using language that is easy to interpret for the target age group.

Features and flexibility: Most tools for the online protection of children rely on parental control. For example, Circle [17] enables control of devices on a home network and enforces limits on screen time, but it does not address user authentication. We specifically propose an authentication mechanism for children that helps achieve password reduction and includes parents in the process. Our scheme offers some autonomy to the child, but still enables parents to have oversight. We envision that most families would configure the system using rules so that the child could login and access pre-approved websites during specified times, giving them autonomy while maintaining boundaries. Some parents felt that even this level of oversight was infringing on the child's privacy. On the other hand, several parents wanted additional parental controls, beyond the scope of an authentication mechanism. These opposing views highlight the vast range of family dynamics and norms, and suggest that any parent-child mechanism needs to accommodate a range of preferences and situations. It is interesting (although perhaps not surprising) to note that children preferred that their parents have a passive role (e.g., being able to check history logs or receive notification of recent logins) but that most parents preferred having a more active role in determining which logins were acceptable.

We found that families rely extensively on mobile devices. Parents frequently had more than one device that they use regularly and wanted access to the *Kindersuf* app from each, as well as needing to coordinate devices between both parents or caregivers. It was clear that the mobile platform was most suited for our parental approval task.

Security risks: Any new authentication mechanism should be assessed for security since a mechanism with security vulnerabilities may fail to meet its intended purpose. Both OpenID and U2F have been extensively evaluated for security [2, 38]. Bonneau et al. [5, 6] have previously proposed the "UDS" (usability-deployability-security) framework for evaluating web-based authentication schemes. 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 and security. Several types of second factor authentication have also been evaluated and show that they are generally better than passwords for security. Our assessment based on the UDS framework is that *KinderSurf* does not introduce any additional significant technical vulnerabilities.

However, a few vulnerabilities are noteworthy, particularly those dealing with human factors. First, *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 impostor. We have discussed the implementation of additional verification checks, such as whether the login requests comes from a known device, or whether the login attempt follows established usage patterns. Exceptions could then be flagged to the parent, overriding any existing rules, and ask for explicit authorization. The parent could then use other communication channels to verify that it is in fact the child logging in.

The impostor might also be a sibling or friend attempting to log in to a child's account, and this was the primary concern of the children in our studies. The optional child password should help with this particular threat.

Another possible vulnerability is that children bypass this system by creating new individual accounts on the websites, instead of logging in with their OpenID credentials. This is of particular concern with older children who may have the knowledge and means to complete such a task. Based on this and other studies that we have conducted, We do not anticipate that younger children would be capable of such deception because most account creation processes require that the user confirms receipt of an email sent to the associated email address, which most younger children do not possess.

Children might be able to gain access to the parent's device used to authorize login requests (e.g., they find Mom's phone) and then authorize themselves. We included the option for parents to have an authorization password on their device, if this threat is of particular concern.

In these last two cases, we note that the threat model has shifted from an unknown online attacker attempting to guess a weak password to an insider threat (in this case, the child themselves). If children have reached a stage where these or other bypass strategies are is feasible, technological barriers are unlikely to stop them. We argue that the protection offered by *KinderSurf* is still improved compared to traditional passwords for web accounts.

Limitations: The main limitation in our studies relate to ecological validity due to prototype limitations and the lab settings. The prototypes and websites were created specifically for testing purposes, and while they included the required functionality, they were not finished products. Furthermore, we conducted our studies in a controlled 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, and their perception of the system may differ, when using the software in day-to-day life compared to the 60 minute session.

Limitations of the proposed *KinderSurf* mechanism include that it is only available on sites which have OpenID authentication enabled. Although limiting, the OpenId community is growing and includes providers like Google and Amazon, so adoption is becoming more widespread.

CONCLUSION

In this paper, we describe our efforts at iteratively designing, prototyping, and testing a parent-child authentication mechanism. Our solution combines OpenID Connect and U2F technology to minimize the password burden for children and provide parents with oversight functionality that is configurable to be as passive or active as appropriate for their family. Parents can use their mobile device to remotely grant or deny login requests from their children, or can configure the system to automatically accept or deny requests for specific websites according to a predetermined schedule. Many parents admitted that they were not initially looking for such a tool but that after interacting with the system, they felt it was needed for their family. With the vast majority of children online from a very young age, age-appropriate authentication mechanisms are critical.

Acknowledgements

This work was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) through an NSERC Engage grant (EGP 495006-16) and the Canada Research Chair Program (Chiasson, 950-231002-2016).

REFERENCES

1. FIDO Alliance. accessed: 2017-1-2a. FIDO Alliance Specifications (UAF and U2F). https://fidoalliance.org/specifications/overview/. (accessed: 2017-1-2).
2. FIDO Alliance. accessed: 2017-1-2b. FIDO Security Reference. https://fidoalliance.org/specs/fido-u2f-v1.1-id-20160915/fido-security-ref-v1.1-id-20160915.html. (accessed: 2017-1-2).
3. Hala Assal, Ahsan Imran, and Sonia Chiasson. 2016. An Exploration of Graphical Password Authentication for Children. *arXiv preprint arXiv:1610.09743* (2016).
4. Australian Bureau of Statistics. accessed: 2016-6-9. Household Use of Information Technology, Australia, 2014-15. http://www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0. (accessed: 2016-6-9).
5. Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. 2012a. *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.
6. Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. 2012b. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*. IEEE, 553–567.
7. Karthik Channakeshava, Kaigui Bian, Michael S Hsiao, Jung-Min Park, Robert E Crossler, France Bélanger, Payal Aggarwal, and Janine S Hiller. 2008. On Providing Automatic Parental Consent over Information Collection from Children. In *Security and Management*. 196–202.
8. Sonia Chiasson, Paul C van Oorschot, and Robert Biddle. 2006. A Usability Study and Critique of Two Password Managers.. In *Usenix Security*, Vol. 6.
9. Brian A Colella. 2010. System for secure internet access for children. (2010). US Patent 7,853,535.
10. Common Sense Media. accessed: 2016-6-9. 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).
11. Daily Mail. accessed: 2017-1-2. More than half of children use social media by the age of 10: Facebook is most popular site that youngsters join. http://www.dailymail.co.uk/news/article-2552658/More-half-children-use-social-media-age-10-Facebook-popular-site-youngsters-join.html. (accessed: 2017-1-2).
12. Mari Ervasti, Minna Isomursu, and Marianne Kinnula. 2009. Bringing technology into school: NFC-enabled school attendance supervision. In *Proceedings of the 8th international conference on mobile and ubiquitous multimedia*. ACM, 4.
13. Gunter Fahrnberger, Deveeshree Nayak, Venkata Swamy Martha, and Srini Ramaswamy. 2014. SafeChat: A tool to shield children's communication from explicit messages. In *Innovations for Community Services (I4CS), 2014 14th International Conference on*. IEEE, 80–86.
14. Federal Trade Commission. 1998. Children's online privacy protection act of 1998. *Center for Democracy & Technology* (1998).
15. Simson Garfinkel and Heather Richter Lipford. 2014. Usable security: History, themes, and challenges. *Synthesis Lectures on Information Security, Privacy, and Trust* 5, 2 (2014), 1–124.
16. Cormac Herley and Paul Van Oorschot. 2012. A research agenda acknowledging the persistence of passwords. *Security & Privacy, IEEE* 10, 1 (2012), 28–36.

17. Circle Media Inc. accessed: 2017-1-2. Circle with Disney. https://meetcircle.com/circle/. (accessed: 2017-1-2).

18. Dale Janssen and Cory Janssen. accessed: 2016-6-9. Techopedia: Password Manager. https://www.techopedia.com/definition/31435/password-manager. (accessed: 2016-6-9).

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

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

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

22. Office for National Statistics. accessed: 2016-6-9. Internet Access – Households and Individuals 2015. http://webarchive.nationalarchives.gov.uk/20160105160709/http://www.ons.gov.uk/ons/dcp171778_412758.pdf. (accessed: 2016-6-9).

23. OpenID Foundation. accessed: 2016-7-26a. Benefits of OpenID. http://openid.net/get-an-openid/individuals/. (accessed: 2016-7-26).

24. OpenID Foundation. accessed: 2016-7-26b. OpenID Connect. http://openid.net/connect/faq. (accessed: 2016-7-26).

25. Jean Piaget. 1952. *The origins of intelligence in children*. Vol. 8. International Universities Press New York.

26. Pumpic. accessed: 2017-1-2. Limitly - Free Screen Time Parental Control App. http://pumpic.com/limitly-parental-app/. (accessed: 2017-1-2).

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

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

29. Natsuhiko Sakimura, J Bradley, M Jones, B de Medeiros, and C Mortimore. 2014. OpenID Connect core 1.0. *The OpenID Foundation* (2014), S3.

30. Linda Smith and Michael Gasser. 2005. The development of embodied cognition: Six lessons from babies. *Artificial life* 11, 1-2 (2005), 13–29.

31. Sampath Srinivas, Dirk Balfanz, and Eric Tiffany. 2015. Universal 2nd factor (U2F) overview. *FIDO Alliance Proposed Standard* (2015), 1–5.

32. Valerie Steeves. 2012. Young Canadians in a Wired World, Phase III: Talking to Youth and Parents about Life Online. (2012).

33. V Steeves. 2014. Life online: Young canadians in a wired world, phase III. *MediaSmarts* (2014).

34. Elizabeth Stobert. 2014. The agony of passwords: Can we learn from user coping strategies?. In *CHI'14 Extended Abstracts on Human Factors in Computing Systems*. ACM, 975–980.

35. The Nemours Foundation. accessed: 2017-1-2. Teaching Kids To Be Smart About Social Media. https://kidshealth.org/en/parents/social-media-smarts.html. (accessed: 2017-1-2).

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

37. Eugene Tsyrklevich and Vlad Tsyrklevich. 2007. Single sign-on for the Internet: a security story. In *Blackhat USA*.

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

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

40. Leah Zhang-Kennedy, Christine Mekhail, Yomna Abdelaziz, and Sonia Chiasson. 2016. From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats. In *Proceedings of the The 15th International Conference on Interaction Design and Children*. ACM, 388–399.