2019

"My Name is My Password:" Understanding Children's Authentication Practices

Dhanush Kumar Ratakonda
Boise State University

Tyler French
Boise State University

Jerry Alan Fails
Boise State University

This document was originally published in *IDC '19: Proceedings of the 18th ACM International Conference on Interaction Design and Children* by Association for Computing Machinery. Copyright restrictions may apply. doi: 10.1145/3311927.3325327

"My Name Is My Password:" Understanding Children's Authentication Practices

Dhanush kumar Ratakonda
Tyler French
dhanushkumarrata@boisestate.edu
tylerfrench@u.boisestate.edu
Computer Science Department
Boise State University
Boise, Idaho

Jerry Alan Fails
jerryfails@boisestate.edu
Computer Science Department
Boise State University
Boise, Idaho

ABSTRACT

Children continue to use technology at an increasing rate, more and more of which require authentication via usernames and passwords. We seek to understand how children ages 5-11 years old create and use their credentials. We investigate children's username and password understanding and practices from the perspective of both children and adults within the context of three security categories: credential composition (e.g. length of password), performance (e.g. time to enter), and credential mechanisms (e.g; a pattern or characters). We conducted a semi-structured interview with 22 children and an online survey with 33 adult participants (parents and teachers) to determine their practices and involvement in facilitating authentication for their children. Our study illustrates how children have a limited understanding of authentication, and that there are differences between children's and adult's understanding of good authentication and security practices, and what they actually do.

IDC '19, June 12–15, 2019, Boise, ID, USA

ACM ISBN 978-1-4503-6690-8/19/06…$15.00
https://doi.org/10.1145/3311927.3325327

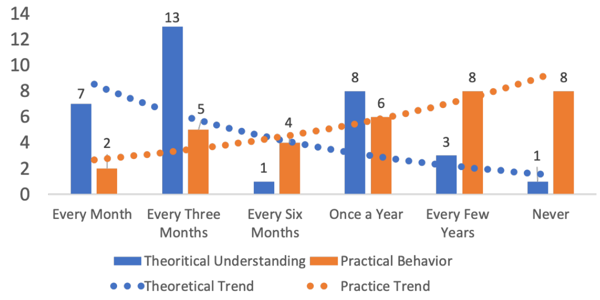

Figure 1: Adult's theoretical understanding versus their actual practices of changing their passwords.

Table 1: Authentication evaluation dimensions with brief definitions and examples.

Category	Dimension
Composition	**Security strength**: e.g. complex character combinations **Self-related**: e.g. child's name
Performance	**Memorability**: e.g. child's name **Error rate**: number of mistakes **Time to enter**: time to successfully authenticate **Shoulder-surfing and sharing**: watching someone enter or telling a password
Mechanisms	**Usage in schools**: how many passwords and mechanisms in school **Reuse**: using the same password in different places **Preference**: overall preferences **Administration**: who administers, how handled

CCS CONCEPTS

• **Human-centered computing** → **Human computer interaction (HCI)**.

KEYWORDS

Authentication for children, security strength, memorability.

ACM Reference Format:

Dhanush kumar Ratakonda, Tyler French, and Jerry Alan Fails. 2019. "My Name Is My Password:" Understanding Children's Authentication Practices. In *Interaction Design and Children (IDC '19), June 12–15, 2019, Boise, ID, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3311927.3325327

INTRODUCTION

It is commonplace to hear of breaches of security that expose large amounts of users or subscribers information. Children use computers, mobile devices, and online applications at an increasing rate. Despite privacy laws protecting children (e.g. COPPA and GDPR), these applications – ranging from leisure activities such as video games, to the software they use at schools – are storing more and more information about children. In addition, breaches in a child's account may lead to breaches in other family member's accounts. As a result, there is a need to create awareness and educate children to secure their electronic accounts via effective authentication protocols – the most common of which is usernames and passwords [2]. As a first step, there is a need for a strong foundation of children's authentication understanding and practices.

In this research, we investigated how elementary school children (ages 5-11) create and use usernames and passwords by conducting semi-structured interviews. Since parents and teachers can have an influence with regards to how children access online systems, we also surveyed adults in these roles as to their: (1) own understanding and practices with regard to authentication, and (2) perceptions of how children understand and utilize authentication mechanisms.

RELATED WORK

A large amount of research has looked at security measures for adults [3, 5–12], and there has been some research conducted with children with regards to security [11, 12] . While these have formed a good foundation, there is a continued need to deepen our understanding of current security practices in order to inform improved future practices. In this study, we look at a broad area of dimensions — that have not collectively been investigated before – specifically looking at authentication. The breadth of authentication categories and dimensions of each are in Table 1. We situate the prior work in relation to these dimensions and further illustrate the need for the research presented later in

Table 2: Responses from child participants: age, children’s preferred character length for username/password, entered alphanumeric username and passwords, the number of applications they use at home and school, number of applications they log into in a week. Gray cells are anonymized with a description provided.

#	Age	Char Length uname/pword	Alphanumeric-Username	Length	Diff
CP22	5	5	[child’s name]	5	0
CP17	6	7	[child’s school login]	9	-2
CP11	7	3	[child’s initials]	1	2
CP8	7	10	[child’s nickname]	6	4
CP6	7	6	[child’s name]	6	0
CP1	8	short	nothing	7	—
CP2	8	4	2010	4	0
CP3	8	7	[child’s name]	14	-7
CP9	8	4	[child’s email]	31	-27
CP10	8	20	0964571hacer	12	8
CP5	8	10	[child’s nickname]	4	6
CP12	8	5	Yogaboy	7	-2
CP15	8	12	lab11134	8	4
CP13	9	11	[child’s name]	9	2
CP14	9	3	[child’s name]	3	0
CP16	9	4	supergirl[name]	14	-14
CP18	9	10	[child’s school login]	9	1
CP4	10	4	serpentine	10	-6
CP20	10	9	[child’s name]	9	0
CP21	10	10	Derpy_Chicken2	14	-4
CP7	11	10	[child’s initials]	6	4
CP19	11	9	[child’s school login]	9	0

#	Alphanumeric-Password	Length	Diff	# Apps	# of Logins in a week
CP22	ariel	5	0	2	0
CP17	d1234	5	2	2	21
CP11	123	3	0	1	3
CP8	[initials & birthday]	8	2	3	5
CP6	tmiewus	7	-1	0	0
CP1	password	8	—	2	Lot
CP2	2810	4	0	1	0
CP3	31589000	8	-1	3	2
CP9	[initials & birthday]	8	-4	2	5
CP10	1bnm	4	16	1	2
CP5	lava	4	6	3	2
CP12	[initials & birthday]	8	-3	4	4
CP15	lab34	5	7	3	21
CP13	[initials & birthday]	8	3	4	12
CP14	4774	4	-1	4	2
CP16	[brother]0314	12	-8	4	50
CP18	fish20816@@	13	-3	4	3
CP4	2018??19	8	-4	0	0
CP20	[child’s name & #]	14	-5	5	15
CP21	petsit123	9	1	6	1
CP7	[garage code]	4	6	3	2
CP19	88597	5	4	2	2

this paper. The most commonly investigated dimensions in the authentication literature related to children are: *memorability*, *security strength*, and *error-rate*.

Read at al. [12] conducted two related studies: one to find out the knowledge children have with regards to passwords and how they use them; and another that investigated the length of characters used by children in their study for usernames and passwords by focusing on *memorability* and *security strength*. They concluded their study with three design implications: length (the length of passwords should be considered), composition (there should be a balance between combinations of numbers, letters, and at the same time being able to remember is an important aspect), and warnings (while creating passwords, there should be four kinds of warning for kids: spellings, repetitive characters, password similar to username, and remembering the start of sequence of numbers).

Lamichhane at al. [8] investigated username and password length with regards to *composition* (both *security strength* and *self-related*) as well as *memorability* in children (aged 7-8). To do this they utilized a game-like interface and asked children a few sets of questions about things which are related to them (children) through an interactive game. At the end of the game, they then asked the children to create a username and password. They asked children to return to the system to enter their already created username and password after an hour of a distraction activity. According to [8], the whole procedure was to see whether children were creating usernames and passwords which are easily guessable, self-related, and memorable [8].

Looking at authentication *mechanisms* Cole et al. [3] compared graphical and textual passwords for children [3]. This study was carried out by asking children (aged 6-12) a set of questions and had children create usernames and passwords for five different sites. Children were given five minutes to play a game as a distraction activity and then were asked to log back into those five different sites. The study revealed that children are more comfortable with creating and recollecting graphical passwords within a short time period even when distracted temporarily. However, the accuracy percentage was greater when participants returned to enter their textual passwords two weeks later. The outcome of this study reveals that authentication using the graphical password mechanism “PassPoint” is problematic for children.

Related to our work in method and generalized topic are is Kumar et al. [7] investigation of privacy concerns for children. In their study they conducted semi-structured interview sessions with both children (*n*=26, ages 5-11) and 23 parents [7]. Their results take a qualitative look at how children (ages 5-7) are not fully aware of privacy policies and their practices, at the same time, older child participants giving wrong information to researchers displayed their security strategy. This illustrates how these children were aware that it is not a good practice for them to share their credentials. These children’s parents were also interviewed to understand their perspectives on privacy and security.

Similar to our study Maqsood at al. Maqsood et al. [9] conducted a study with children aged 11 to 13 years (n = 20). Their main goal is to understand how children are creating passwords to secure their information. They used three different websites with three different rules to create passwords. Based on the rules to create passwords they referred those websites as "low", "medium", and "high" complexity. Participants in their study

took more time to create their passwords in medium and high complexity websites compared to low complexity website. They note that children had no memorability issues when re-entering their passwords, participants created very easy passwords and believed that it would be impossible for a stranger to guess their passwords.

As indicated above, prior security research for children has not evaluated all of these dimensions together in a single study for children ages 5-11. Since security is multi-faceted, we posit that this more holistic approach provides can lead to better security practices. The main goal of our research is to better understand the authentication practices of children and the perceptions and influence of adults (parents and teachers) on children's understanding and practices. After attaining the approval form Institutional Review Board (IRB) we conducted semi-structured interviews for child participants and online survey with adults. An overview of both (interview and servery) is provided in Table 3 and Table 4. Next we present our analysis and discussion.

Table 3: Child interview structure, conducted with 22 children (ages 5-11).

Segment 1. children were asked to enter an alphanumeric username and password with no length or character combination restrictions.
Segment 2. I asked them to create a pattern passcode using the basic Android-pattern mechanism. A screenshot was used to capture the password they entered.
Segment 3. Sixteen open-ended questions that related to the security dimensions above (main categories include composition, performance, mechanism) were asked to children. Notes were taken on their responses and they were also recorded and transcribed.
Segment 4. Children were asked to create a numeric password using the Android number passcode mechanism. A screenshot was used to capture the password they entered.

Table 4: Adult's online survey structure, conducted with 33 adults (25 parents, 5 teachers, 3 both parents and teacher)

Online survey consisted of questions about: demographics, the adult's authentication understanding and practices, and how the adult is involved in authentication practices for children in their stewardship.
In our first section of the survey, we asked several questions which are related to the dimensions in Table 1 and few demographic questions.
The second section of the *adult* survey consisted of questions to evaluate the general security behaviors of adults. To do this we utilized the Security Behavior Intentions Scale (SeBIS) [5].

ANALYSIS AND DISCUSSION

The analysis was conducted using an inductive approach to develop codes and categories by the authors reviewing the transcribed children's responses to the semi-structured interviews and typed adult survey responses [1, 4]. For ease of referencing we will refer to child participants as CP. In the remainder of this section we discuss the responses to the questions in relation to the dimensions previously described.

Composition

Security Strength. We asked adults "What combination of characters makes a good password?" and 100% of our adult participants (33 of 33) indicated the importance of combinations of elements (e.g. letters, numbers, and/or special characters) in their passwords. When children, were asked "What do you think makes a good password in terms of being a strong password?" 54% of child participants (12 of 22) mentioned the need to include combinations of numbers, letters, and/or special characters; 14% (3 of 22) mentioned the need to randomly arrange characters when creating a good password. The collected data from children about their password character lengths illustrates a mismatch between their understanding and practice (see 'Diff' in Table 2). In many cases, the username or password is *anonymized* so as to not reveal information about the participants because they were related to the participants fitting within the composition dimension of *Self-Related.*

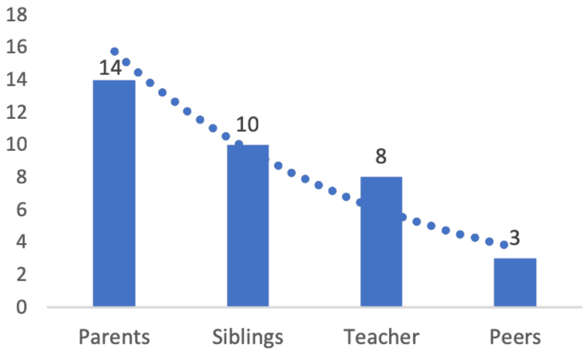

Figure 2: Child participant’s opinion on sharing credentials.

Performance

Memorability. When child participants were asked “Do you use any tool to save your usernames and passwords?”, 54% (12 of 22) of child participants indicated they use a tool for saving their credentials. Also, 45% (15 of 33) adult participants replied that they *(adults)* use a piece of a paper as a tool for saving their credentials, this corroborates with the children’s response “write them on a paper”. As illustrated in

Error rate. When children were asked “Has one of your accounts ever been locked due to entering your password wrong too many times?” 45% (10 of 22) child participants said their accounts got locked. A similar question was asked of adults, and 67% (22 of 33) replied that their devices had been locked at least one to two times due to children entering their credentials wrong multiple times.

Time taken to enter. We asked adults “How long does it take for your child to enter their username and passwords?” 36% (12 of 33) of adult participants answered their children would take “11-20 seconds” to enter their credentials however, from the researchers observation in semi-structured interview sessions children took more than “11-20” seconds to enter their credentials.

Over the shoulder and sharing. When children were asked to create an alphanumeric, pattern, and numeric passwords they readily did so in the researcher’s presence and were not at all bothered about researchers watching them create and enter their credentials. This could be due to the fact that the children trusted the researchers or were making an exception, or it could be that children are less aware of how others can learn a password by watching them. Interestingly, when we asked adults “How concerned are your children entering their credentials in the presence of someone?” 61% (20 of 33) of adult participants said their children are concerned. 68% (22 of 33) of child participants said they would share their usernames and passwords with someone close to them. For the question “Do you share your username and password to someone close to you?” Responses of the child participants are depicted in the Figure: 2

Mechanisms

Usage in schools. We asked children “what are the different applications you use at school?” and 77% (17 of 22) participants responded that they use at least one. When adults were asked “Do teachers talk to children about how to create usernames and passwords?”, 36% (12 of 33) of participants said teachers talk to children about how to create usernames and passwords.

Re-use. When children were asked “Do you use the same username and password for all the applications you login to?” 63% (14 of 22) said that they would not reuse them for different applications. 42% (14 of 33) adults responded to this question as children sometimes reuse their credentials and 27% (9 of 33) participants responded that children always reuse their credentials. Most of the adults responses for *re-use* evaluation dimension illustrate that children and adults frequently reuse their credentials due to memorability issues. We also asked adult participants about their own understanding and practices. In theory, they understood the need to change the credentials, but in practice they did not do it as frequently as they said they should in theory. See Figure: 1 for the difference between the adult's theoretical understanding versus their actual practice in changing their authentication credentials.

Preference. 82% (18 of 22) of child participants said they would prefer alphanumeric password mechanism over pattern and number password mechanisms. Two participants said they never had an interaction with pattern mechanism and two said they would prefer pattern as it is very fast and easy to remember in their perception.

Administration. In terms of general administrative practices related to authentication, we asked adults "Do you as a teacher or parent play any role in creating your children's passwords?" 77% (25 of 33) of adult participants replied in the affirmative and 68% (17 of 25) of the adult participants replied that either they create credentials for their children or they worked with their children to create them. This reveals that adults play an important role in creating credentials for their children.

CONCLUSION AND FUTURE WORK

In this paper we presented the results from interviews of children and a survey of adults that elucidates children's understanding and practices with regards to authentication. Most of the children and adults in this study have a theoretical knowledge about the credentials creation and usage but do not implement that knowledge in their practices. There is a large discrepancy in the number of characters they would want in their credentials and the number of characters children actually included when they asked to create one, this impacts the *security strength* of their authentication. Future work includes, understanding children and adult practices further by continuing to investigate the authentication dimensions of composition, performance, and mechanisms. Further understanding may lead to the need to design a password mechanism that better meets children's specific needs as well as maximizes the efficiency of the authentication mechanisms they use.

ACKNOWLEDGMENTS

We thank the children and adults who participated in this study for their valuable input.

REFERENCES

[1] Kathy Charmaz and Linda L. Belgrave. 2012. Qualitative interviewing and grounded theory analysis. *The SAGE Handbook of Interview Research: The Complexity of the Craft* (Jan. 2012), 347–366. https://doi.org/10.4135/9781452218403.n25

[2] Sonia Chiasson, Alain Forget, Elizabeth Stobert, P. C. van Oorschot, and Robert Biddle. 2009. Multiple Password Interference in Text Passwords and Click-based Graphical Passwords. In *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09).* ACM, New York, NY, USA, 500–511. https://doi.org/10.1145/1653662.1653722

[3] Jasper Cole, Greg Walsh, and Zach Pease. 2017. Click to Enter: Comparing Graphical and Textual Passwords for Children. In *Proceedings of the 2017 Conference on Interaction Design and Children - IDC '17.* ACM Press, Stanford, California, USA, 472–477. https://doi.org/10.1145/3078072.3084311

[4] John W. Creswell. 1998. *Qualitative inquiry and research design: choosing among five traditions.* Sage Publications.

[5] Serge Egelman and Eyal Peer. 2015. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 2873–2882. https://doi.org/10.1145/2702123.2702249

[6] Tatiana Gossen, Juliane Hobel, and Andreas Nurnberger. 2014. A Comparative Study About Children's and Adults' Perception of Targeted Web Search Engines. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 1821–1824. https://doi.org/10.1145/2556288.2557031

[7] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2017. 'No Telling Passcodes Out Because They're Private': Understanding Children's Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (Dec. 2017), 1–21. https://doi.org/10.1145/3134699

[8] Dev Raj Lamichhane and Janet C. Read. 2017. Investigating Children's Passwords using a Game-based Survey. In *Proceedings of the 2017 Conference on Interaction Design and Children - IDC '17*. ACM Press, Stanford, California, USA, 617–622. https://doi.org/10.1145/3078072.3084333

[9] Sumbal Maqsood, Robert Biddle, Sana Maqsood, and Sonia Chiasson. 2018. An exploratory study of children's online password behaviours. In *Proceedings of the 17th ACM Conference on Interaction Design and Children - IDC '18*. ACM Press, Trondheim, Norway, 539–544. https://doi.org/10.1145/3202185.3210772

[10] Diogo Marques, Luís Duarte, and Luís Carriço. 2012. Privacy and secrecy in ubiquitous text messaging. In *Proceedings of the 14th international conference on Human-computer interaction with mobile devices and services companion - MobileHCI '12*. ACM Press, San Francisco, California, USA, 95. https://doi.org/10.1145/2371664.2371683

[11] Janet C Read and Russell Beale. 2009. Under my pillow: designing security for children's special things. (2009), 5.

[12] 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 (IDC '12)*. ACM, New York, NY, USA, 200–203. https://doi.org/10.1145/2307096.2307125