Toward Understanding Children's Use and Understanding of User Authentication Systems: Work-in-Progress

Tempestt Neal*, Lisa Anthony+, Shaun Canavan*, Jaime Ruiz+, Saandeep Aathreya*,
Meghna Chaudhary*, Yu-Peng Chen+, Heting Wang+, Rodrigo Calvo+, Liza Jivnani*, Nicolas Ng Wai*
*University of South Florida, +University of Florida

Abstract

Children's use of computing devices has increased over the past 15 years, requiring age-appropriate user authentication systems. This paper details a research study which investigates continuous authentication systems that do not require user-initiated interactions as an accessible authentication model for not only children users, but users across different age groups, with specific application on personal computing devices.

1 Introduction

The use of computing devices by children has grown significantly [1]. Meanwhile, a person's age impacts their vulnerability to security and privacy risks [3]. Although user authentication systems act as an initial security checkpoint when accessing a device [2,7], current authentication systems (i.e., knowledge-based (*what the user knows*), token-based (*what the user has*), or biometrics-based (*who the user is*)) are not readily usable by children. For example, research [4,5,9] investigating knowledge-based systems for children suggests that children recognize the purpose of authentication systems, but may face difficulties with recalling and spelling their passwords. More generally, "few studies have explored age-related performance across authentication systems" [6].

Continuous authentication (CA) has been proposed to solve the challenges with authenticating [8]. In CA, the device's sensors track the user's multimodal behaviors passively to use all possible signals as input for authentication, no longer requiring user-initiated interactions. This work-in-progress paper describes an ongoing collaborative study conducted at the University of South Florida and University of Florida which investigates the impact of age on users' understanding and use of authentication systems, with a longer term goal of developing age-aware CA systems to help counter the challenges faced by users of different age groups. This paper details our study design, including qualitative and quantitative procedures. We also briefly overview challenges encountered thus far and plans for future work.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022.
August 7–9, 2022, Boston, MA, United States.

2 Study Design

This project investigates the design and usability of age-aware CA through user studies and pattern recognition tasks. These tasks have received Human Subjects approval by the University of South Florida (STUDY002291) and University of Florida (IRB202100450) Institutional Review Boards (IRBs).

User Studies By applying human-centered computing strategies [10], we are conducting a series of focus groups to elicit the mental models users have of user authentication systems. These focus groups include design probes, such as a short video that provides an animated example of a family using CA in their home (see Figure 1). Participants are encouraged to elaborate on any notable frustrations they have experienced that may be unique to people in their age group, among other topics. In addition, a goal of the focus groups is to identify use cases and specific experiences to ask about in a broader-scale survey (hundreds of survey respondents). Survey topics will explore participant perceptions around the uncertainty of what data is collected and who has access to the data stored by such devices. This is important given that CA systems passively collect and analyze a wide range of data. At the conclusion of this task, data will be analyzed to understand user expectations and needs for authentication that can be applied to the design of CA-based systems.

Pattern Recognition Another key task is dataset development to facilitate user authentication experiments. Consenting

Figure 1: Clip from an animated video that demonstrates the use of continuous authentication on smart devices in a home setting. In this segment of the video, a child is attempting to edit a grocery list that has been populated on a smart refrigerator; however, the refrigerator uses voice recognition to determine that the child user is not an authorized user of this service and denies the request.

children and adults are brought into the lab to complete a set of tasks using a Lenovo ThinkCentre M710 workstation, a OnePlus Nord N10 5G smartphone, and while wearing an Empatica E4 wrist-worn wearable. The lab environment, shown in Figure 2, is similar to that of a home setting to encourage natural interaction with the devices. During each session, various physical, physiological, and behavioral signals are gathered transparently.

With this dataset, our main objective is to marry the defined qualitative and quantitative research tasks to develop usable user-centric authentication systems for users across many age groups that

- provide age-appropriate transparency;
- advance understanding of users' mental models for usable privacy and security;
- enable users to create accurate mental models of authentication systems' contexts and states;
- and inform future research directions for on-device CA.

Thus, next steps involve utilizing outcomes from our focus groups and survey to inform the interfaces of new age-aware user authentication systems that are trained using the appropriate pattern recognition techniques (e.g., many-to-one deep sequence models that output an authentication decision given prior user behaviors or physical/physiological signals as input), leading to interactive security experiences.

Figure 2: Research lab setup that mimics a living environment in a home for data collection.

3 Research Challenges

Identifying age-appropriate data collection tasks and editing the language of human subjects forms to ensure children understand the research context and their involvement presented initial challenges when launching this project. Navigating these challenges required several iterations of our IRB documents. For example, one notable change included simplifying the language of the child assent form to define research as follows.

> *We would like for you to participate in a research study. In a research study, a group of people work together to answer a question. For example, let's say you received a new lunchbox, and you want to know how many containers it will hold. To find out, you pick out three containers of different sizes: a small container, a medium-sized container, and a large container. Eventually, you figure out that the lunchbox can hold two small containers and one medium-sized container. This example is similar to a research study. You wanted to know "how many containers will the lunchbox hold?" This is called a research question. To answer the research question, you tried different ways of filling the lunchbox until you were able to find the answer to your research question.*

We also had to carefully think through communicating the context of our research study, and why we need children to participate:

> *If you or someone you know uses a computer or phone, you may have to enter a password or use your finger to unlock the computer or phone before*

you can use it. There are different ways to unlock a computer or phone, so our research question is "what is the best way for children to unlock their computers and phones?"

We have also faced difficulty recruiting children for data collection by inviting children/family members of adult participants, sending the study advertisement to local elementary schools, and leveraging word of mouth. Thus, immediate efforts focus on developing age-appropriate study recruitment materials.

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grants No. 2039373 and 2039379. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

[1] Brooke Auxier, Monica Anderson, Andrew Perrin, and Erica Turner. Parenting children in the age of screens. *Parenting Children in the Age of Screens*, Dec 2020. https://www.pewresearch.org/internet/2020/07/28/parenting-children-in-the-age-of-screens/.

[2] PA Grassi, M Garcia, and J Fenton. Nist special publication 800-63-3 revision 3 digital identity guidelines. *National Institute of Standards and Technology, Los Altos, CA*, 2019.

[3] Ros Hill, Vicky Lewis, and George Dunbar. Young children's concepts of danger. *British Journal of Developmental Psychology*, 18(1):103–119, 2000.

[4] Porter E. Coggins III. Implications of what children know about computer passwords. *Computers in the Schools*, 30(3):282–293, 2013.

[5] Sumbal Maqsood, Robert Biddle, Sana Maqsood, and Sonia Chiasson. An exploratory study of children's online password behaviours. In *Proceedings of the 17th ACM Conference on Interaction Design and Children*, pages 539–544, 2018.

[6] James Nicholson, Lynne Coventry, and Pam Briggs. Faces and pictures: Understanding age differences in two types of graphical authentications. *International journal of human-computer studies*, 71(10):958–966, 2013.

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

[8] Sanka Rasnayaka and Terence Sim. Who wants continuous authentication on mobile devices? In *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–9, 2018.

[9] Janet C. Read and Brendan Cassidy. Designing textual password systems for children. In *Proceedings of the 11th International Conference on Interaction Design and Children*, IDC '12, page 200–203, New York, NY, USA, 2012. Association for Computing Machinery.

[10] Nicu Sebe. *Human-centered Computing*, pages 349–370. Springer US, Boston, MA, 2010.