The Effect of New NIST Password Guidelines on Password Creation For Web Applications and a Comparison to The Past
(Technical Paper)

How Elementary Age Children Learn To Use Digital Technology
(STS Paper)

A Thesis Prospectus Submitted to the

Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree
Bachelor of Science, School of Engineering

Vinh Do
Spring, 2021

Technical Project Team Members
Vinh Do

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature ___*Vinh Do*_____ Date __5/5/21__
Vinh Do

Approved _____ Date _____
Aaron Bloomfield, Department of Computer Science

Approved _____ Date _____
Bryn Seabrook, Department of Engineering and Society

Introduction

"The password you entered is incorrect. Please try again." These two sentences are a common and annoying sight in the digital age. The average user has 25 password-locked accounts, and will use eight of them a day (Yıldırım & Mackie, 2019). Password creation rules are a fairly universal process; the password must include a minimum number of characters and possibly a capital letter and/or a special character. Despite these simple requirements, password management becomes difficult when several applications all require passwords with a distinct set of requirements and no justification for why, making it nearly impossible for the average user to keep track of which passwords belong where. Users are then left with the dilemma of trying to create a password that fits the specific requirements while still being memorable enough to recall later (Yıldırım & Mackie, 2019). Analyzing previous research about how these requirements differ between applications as well as replicating a previous experiment using current examples could reveal a pattern to these seemingly random requirements and help users to not only make stronger passwords but to also keep track of them all.

An even greater barrier to using technology is the skills to navigate through a computer interface and to manipulate physical hardware. In the modern day, technology evolves multiple times in a generation, causing children to grow up with technology that their parents may not have ever used before. Just in the past two decades, Apple's technology has gone from the iPod, whose sole purpose was to play music, to the iPhone X, a smartphone showcasing facial recognition and haptic touch technology (Wallace, 2020). In the case of touchscreens, some children are easily able to transfer their understanding of physical gestures into their digital impacts, but certain methods of instruction have been shown to be more effective than others (Hiniker et al., 2015). These methods will be explored to determine how young children learn to

use technology with the ultimate goal of being able to capitalize on this research in order to design more effective technology for the age demographic. The findings of these two investigations will be documented in two research papers, each with further analysis on the research's impacts on society.

Technical Topic (Capstone)

Every aspect of digital life is guarded by a login requiring a username and password. From financial transactions to long-distance communication to recreational entertainment, having an account with a password is a prerequisite to living in the digital age. The number of passwords necessary to navigate through the digital world can be overwhelming, resulting in around 99% of users reusing existing passwords due to it being too difficult to remember them all (Swinhoe, 2020). This behavior places the burden of maintaining security on the application developers who, rather than store each password directly, store a hash of the password, a string of characters that is deterministically generated from the inputted password (Kumar, 2017). When a user inputs a password in an attempt to log in, the entered phrase is sent through the same hashing algorithm and the result is compared to the stored hash in the database. The two most popular hashing algorithms are MD5 and SHA, however vulnerabilities within MD5 were discovered recently, so now MD5 is only used for functions that do not heavily depend on security, such as ensuring a download has not been tampered with (Kumar, 2017; Nakov, 2019). The first variant of SHA (SHA-1) has been cracked, however the next two versions, SHA-2 and SHA-3, are still used and even recommended by the United States government (Nakov, 2019). When malicious actors try to break into a system, two popular methods are the brute force method and what is known as a dictionary attack (Swinhoe, 2020). The brute force method involves trying every possible combination of characters to try to guess a password, while a

dictionary attack involves running through an exhaustive list of commonly used or related words and phrases (Swinhoe, 2020). Studies have shown that an effective way of defending against these attacks would be to simply increase the number of characters in a password, outweighing the benefit of including an uppercase letter or a special character (Mayer et al., 2017). Users interested in creating secure passwords could follow this advice; however some applications still have requirements for different case letters and special characters, increasing the complexity of the password and decreasing the chance that a user will be able to recall it in the future.

In order to study how these techniques are used in the real world, this technical project will consist of a modified version of an experiment in which researchers studied the minimum password requirements for several internet applications and compared them to each other based on attributes of the websites, such as the purpose of the site and the presence of advertisements (Mayer et al., 2017). The data collected in this experiment was collected up to 2016, however, in 2017 the National Institute of Standards and Technology released new password restriction guidelines for applications to follow, so one goal of the research will be to determine the effect of the new guidelines (Yıldırım & Mackie, 2019). Alongside the experiment, other research papers will be used to discover possible explanations for the results of the changes, or lack of, and the final product will be a synthesis of all the research in order to determine exactly what is necessary to create a new password in the hopes that users will be able to use this information to remember the passwords for all their accounts.

STS Topic

Having grown up with technology, children today are expected to be technologically-savvy and digitally literate. The integration of technology into elementary learning and the early developmental years has introduced children to digital screens and

electronic devices earlier than previous generations, who had already matured by the time these technologies were adopted (Dong et al., 2020). With online learning being used extensively during the pandemic, the need for children to be technologically literate is greater than ever before (Dong et al., 2020).

It is easy to imagine an adult reading through instructions on how to use the latest iPhone, but how can a toddler who cannot yet read figure out how to navigate the user interface of a thin piece of metal? Studies show that by age 8, children are fully capable of navigating an application with a computer mouse and a keyboard, so although it is known that these skills have already developed by early elementary school, the exact process of how children obtain these skills is not yet well-defined (Yan & Fischer, 2004). Previous research has found various features that, when included in an application, aid children in navigating a website or learning how to use a new user interface, however the justifications for their effectiveness has not yet been fully explored (Lim et al., 2012). Further exploration of the mental and physical processes that accompany this type of learning will benefit parents, teachers, and engineers developing technology for children. Identifying the most efficient way to teach children how to use a laptop or a computer allows parents and teachers to more-easily prepare elementary-age children for success in the future. One common technology given to students in American schools is a Chromebook, a laptop that runs on Chrome OS, which makes up 1.1% of the OS market (Fowler & Fowler, 2020; Vaughan-Nichols, 2020). When compared to iOS, Windows, and Android systems, which make up approximately 30% of the market each, there is a possibility that starting students off with this narrow view of technology could hinder their understanding of more commonly used systems in the future (Vaughan-Nichols, 2020). The results of such a

hypothesis could be revealed through identifying how exactly children are learning how to use this technology and if that learning can be applied to other similar scenarios.

The Social Construction of Technology (SCOT) framework dictates that technological development is determined by its relevant social groups and the compromises that they make with each other to appeal to each group's interests (Klein & Kleinman, 2002). This STS framework is used to analyze how society and its beliefs influence technological development, however a common critique is that not all social groups are always able to be represented, resulting in some opinions being unaccounted for (Klein & Kleinman, 2002). A remedy to this critique would be to bring attention to underrepresented social groups so that their voices are heard, which is an indirect effect of this research due to the increased analysis of a social group which often does not have the maturity to voice their opinions, elementary age children. Using this framework to analyze the research will help engineers and developers to better understand the factors that play into children's technological learning, thus enabling them to create tools and toys that are better suited to the capabilities of certain age groups, as well as applications that can build off of what children already know in order to teach them even more.

Research Question and Methods

How do elementary-age children learn to use and interact with digital technology and how can this information be used to aid designs for children? The answer to this research question will be explored through two main methods: documentary research methods and discourse analysis. Answers to this question will come from analyzing several existing sources of research and synthesizing an overall conclusion that encompasses all the various ways in which children learn to use technology at a young age. Research papers detailing prior experiments and other papers that combined multiple sources will make up most of the resources used to answer

this research question. As for discourse analysis, articles from experts in the field will also be integrated into the final product to formulate an answer to the research question. As previously stated, by age 8, children have developed the necessary skills to use a computer and a mouse, so the research focus will be on children age 8 and younger, as they are more likely to demonstrate observable processes of learning new technologies. A key phrase that will be used for initial research is "children learning digital technology" and afterwards, the research will follow any leads based on the results of such a search. These two methods are well-suited to answering the research question because of their ability to synthesize a bigger argument by combining multiple sources together which allows for the research question to be answered in multiple ways to reflect the multiple pathways that children could take to learning a new digital technology.

Conclusion

The technical capstone project will replicate existing research using modern applications in order to observe any changes over time from recent developments in technology and policy. This replication serves to determine the effects of these developments as well as possibly discovering a solution to the multitude of passwords that digital users must keep track of everyday. Completing this research would allow for developers to observe the effectiveness of introducing new password creation regulations and for digital citizens to traverse the multitude of accounts they possess more easily. The STS research paper will return a description of methods that elementary-age children employ when attempting how to use a foreign piece of digital technology. With these findings, developers of technology will be able to make more informed decisions when designing for children and will thus be capable of creating more effective software and hardware for the intended demographic.

References

Technical Report (Capstone) References

Chiasson, S., Forget, A., Stobert, E., van Oorschot, P. C., & Biddle, R. (2009). Multiple password interference in text passwords and click-based graphical passwords. *Proceedings of the 16th ACM Conference on Computer and Communications Security - CCS '09*, 500. https://doi.org/10.1145/1653662.1653722

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K., & Theofanos, M. F. (2017). *Digital identity guidelines: Authentication and lifecycle management* (NIST SP 800-63b; p. NIST SP 800-63b). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63b

Kumar, S. (2017, April 9). How to store a password in database? *GeeksforGeeks*. https://www.geeksforgeeks.org/store-password-database/

Luna, K. (2019). If it is easy to remember, then it is not secure: Metacognitive beliefs affect password selection. *Applied Cognitive Psychology*, *33*(5), 744–758. https://doi.org/10.1002/acp.3516

Mayer, P., Kirchner, J., & Volkamer, M. (2017). *A Second Look at Password Composition Policies in the Wild: Comparing Samples from 2010 and 2016*. https://www.usenix.org/system/files/conference/soups2017/soups2017-mayer.pdf

Nakov, S. (2019). *Secure Hash Algorithms*. Practical Cryptography for Developers. https://cryptobook.nakov.com/cryptographic-hash-functions/secure-hash-algorithms

National Institute of Standards and Technology. (n.d.). [Text]. NIST. Retrieved November 6, 2020, from https://www.nist.gov/

NIST Password Guidelines. (2019, November 18). Solarwinds MSP. https://www.solarwindsmsp.com/blog/nist-password-standards2

Swinhoe, D. (2020, August 5). *What is a dictionary attack? And how you can easily stop them*. CSO Online. https://www.csoonline.com/article/3568794/what-is-a-dictionary-attack-and-how-you-can-easily-stop-them.html

Yıldırım, M., & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, *18*(6), 741–759. https://doi.org/10.1007/s10207-019-00429-y

STS Research References

Bird, J., & Edwards, S. (2015). Children learning to use technologies through play: A Digital Play Framework. *British Journal of Educational Technology*, *46*(6), 1149–1160. https://doi.org/10.1111/bjet.12191

Dong, C., Cao, S., & Li, H. (2020). Young children's online learning during COVID-19 pandemic: Chinese parents' beliefs and attitudes. *Children and Youth Services Review*, *118*, 105440. https://doi.org/10.1016/j.childyouth.2020.105440

Fowler, G. A., & Fowler, G. (2020, August 10). Perspective | Back-to-school laptop guide: Pandemic survival edition. *Washington Post*. https://www.washingtonpost.com/technology/2020/08/10/laptop-buyers-guide-distance-learning/

Hiniker, A., Sobel, K., Hong, S. R., Suh, H., Irish, I., Kim, D., & Kientz, J. A. (2015). Touchscreen prompts for preschoolers: Designing developmentally appropriate techniques for

teaching young children to perform gestures. *Proceedings of the 14th International Conference on Interaction Design and Children - IDC '15*, 109–118. https://doi.org/10.1145/2771839.2771851

Hossain, M. A., Sormunen, E., Aparac-Jelušić, T., & Kurbanoglu, S. (2019). Does informal peer learning stimulate acquisition and development of ICT skills? *Education for Information*, *35*(2), 129–148. https://doi.org/10.3233/EFI-180241

Klein, H. K., & Kleinman, D. L. (2002). The Social Construction of Technology: Structural Considerations. *Science, Technology, & Human Values*, *27*(1), 28–52. https://doi.org/10.1177/016224390202700102

Lauricella, A. R., Barr, R. F., & Calvert, S. L. (2008). Emerging Computer Skills: Influences of Young Children's Executive Functioning Abilities and Parental Scaffolding Techniques. *Conference Papers -- International Communication Association*, 1–31.

Lim, C., Song, H.-D., & Lee, Y. (2012). Improving the usability of the user interface for a digital textbook platform for elementary-school students. *Educational Technology Research and Development*, *60*(1), 159–173. https://doi.org/10.1007/s11423-011-9222-5

Lundtofte, T. E. (2020). Young Children's Tablet Computer Play. *American Journal of Play*, *12*(2), 216–232.

Martens, M. (2012). Issues of access and usability in designing digital resources for children. *Library & Information Science Research*, *34*(3), 159–168. https://doi.org/10.1016/j.lisr.2011.12.003

Mineshita, Y., Kim, H.-K., Chijiki, H., Nanba, T., Shinto, T., Furuhashi, S., Oneda, S., Kuwahara, M., Suwama, A., & Shibata, S. (2021). Screen time duration and timing: Effects

on obesity, physical activity, dry eyes, and learning ability in elementary school children. *BMC Public Health*, *21*(1), 1–11. https://doi.org/10.1186/s12889-021-10484-7

Norman, D. A. (2013). *The design of everyday things* (Revised and expanded edition). Basic Books.

Palaiologou, I. (2016). Children under five and digital technologies: Implications for early years pedagogy. *European Early Childhood Education Research Journal*, *24*(1), 5–24. https://doi.org/10.1080/1350293X.2014.929876

Technology and Young Children in the Digital Age. (2016). Erikson Institute. https://www.erikson.edu/wp-content/uploads/2018/07/Erikson-Institute-Technology-and-Young-Children-Survey.pdf

Vaughan-Nichols, S. J. (2020, May 6). *Most popular operating systems of 2020: The more things change...* ZDNet. https://www.zdnet.com/article/whats-2020s-most-popular-operating-systems/

Wallace, I. (2020, May 28). *Apple History Timeline [Infographic]*. Infographic Journal. https://infographicjournal.com/apple-history-timeline/

Yan, Z., & Fischer, K. W. (2004). How children and adults learn to use computers: A developmental approach. *New Directions for Child & Adolescent Development*, *2004*(105), 41–61. https://doi.org/10.1002/cd.110

Yogman, M., Garner, A., Hutchinson, J., Hirsh-Pasek, K., Golinkoff, R. M., Health, C. on P. A. of C. and F., & Media, C. on C. A. (2018). The Power of Play: A Pediatric Role in Enhancing Development in Young Children. *Pediatrics*, *142*(3). https://doi.org/10.1542/peds.2018-2058