Investigating Password Security and Accessibility

Jared B. DeWinne

Professor Adams

Saint Leo University

December 3, 2018

Table of Contents

Abstract

This research paper reflects a question of "How can you convince users to care about password security, yet still allow the ease of access to remaining the same, if not better?" The question of access is one that will not be answered entirely, as it is an ongoing question, hopefully, to be challenged and updated as time goes on. Password managers, password requirements, and such related topics will be discussed and identified, while questioning their value in an everyday use setting, from quality to quantity.

Keywords: Password, Security, Saint Leo University, Facebook, requirements, Information Security

Investigating Password Security and Accessibility

Introduction

For my research project for COM-203, I am diving into the issue of passwords for needed users. As most people know, the backbone of internet security as we know it is an encryption of some sort when all boiled down is a type of password or passphrase. Recent studies have shown statistics on the requirements for these security measures and I will be exploring further into this field.

Statement of Problem/Background

In an age filled with clickbait, and "Press me to get an extra life!" we are filled with constant notifications that deter us from our original quest online. With all these different sites, you have different password requirements. "7-11 letters with at least one number and at least one symbol", you end up with a variety of different passwords, for a variety of various sites. For the average grandma, having "P@ssw0rd" as their Facebook password where they post pictures of their favorite denture cleaners, they believe no hacker will ever be able to reach granny's sophistication level. Little does she know; the average script kiddie can break that password in a matter of seconds. But where the problem arises; why should she care? She believes she is protected, and who would want access to her information? This is where the average user lacks the advanced knowledge of internet security, where the problem exists.

Objectives

I aim to correctly and vividly find and show this topic to its maximum capability and allow it to be an on-going study. This will be possible with the correct research, summaries, course of action, and afterward thoughts. While it will be challenging to conduct data on my own, I must use the data already existing as much as possible. I would like to have a way for this

research to be continuously updated, as this situation is a continually updated one. I will demonstrate, using both text and graphics, information that will allow a solution to be proven. After these demonstrations, I will heavily focus on the discussion and need for more research to be done. Even if I can gather my statistics, this needs to be brought widescale and needs to be emphasized by security experts. Once understanding the problem, current understanding status, and seeing potential solutions an onlooker should be inclined to partake in answer to this issue.

Core Value: Personal Development

The core value of this research topic for this computer science class has to do with is personal development. "Saint Leo University stresses the development of every person's mind, spirit, and body for a balanced life. All members of the Saint Leo University community must demonstrate their commitment to personal development to help strengthen the character of our community" (saintleo.edu). With this value in mind, educating yourself on this topic will allow you always to think when regarding issues related to internet security for the future.

Plan of Action

1) Gather further in-depth research already existing
    a. Locate quality works and examine thoroughly
    b. Find and show relevance to related research
2) Use research in own paper
    a. Correctly annotate, describe, and cite related information
    b. Use parts in paper to guide discussion and demonstrations
3) Open for future discussion
    a. Offer rhetorical based questions that needs critical thinking

b. Identify accessibility routes, potential solutions, plans on how to achieve solutions
c. Put into action
d. Begin research on action

Conclusion

While not yet answered, this paper reflects a bigger question, one with no end. How can we as Network Administrators and security experts increase the security in all applications without taking away the accessibility for the standard user? My answer is this: we investigate what is going on right now, we identify possible solutions, we use what we found to create a solution that does not negatively affect users in any way. By following those three main thesis steps, we will have created a platform where everyone is secure, and everyone is happy.

First, identification of what is going on is the beginning. We need a proper understanding of why things are the way they are, and what users are doing to protect themselves. Without this information, our data won't matter numbers don't matter, but people do. We need a proper way to collect this information, so it differs from other data, but still is a foundation for the project to come.

Second, we need to identify possible solutions to our problem. While it is easy to require users to use 50 characters and two-factor authentication, that is not the easiest for the everyday user — perspective matters when viewing potential items that can affect the mainstream users. So, we need to look at solutions that will be reasonable in a factor and is accomplishable. New platforms can appear, but we should try to deviate from "reinventing the wheel" as the wheel has been turning for decades.

Lastly, we need to identify and capture common ground. By doing this, we will create a platform that has a solution to our problem and does not negatively affect the typical user. This

common ground is the least technical aspect of the entire project, yet the most important. This step needs to have consideration as it is crucial for any form of success.

While this may seem as if any solution exists only in fantasy, there is the opportunity for attempts of success. Failed attempts will help in the long run to make a platform that benefits all and indeed promotes good in the world of technology. The three main steps are the identification of our problem, solution, and common ground. Evergrowing and neverending projects such as these do exist, and without them, there would be no innovation, no change, and no improvement in the world we live in today.

References

Arora, M. (2004). E-Security Issues. *International Journal Of Computers & Technology, 3*(2c), 301-308. doi:10.24297/ijct.v3i2c.2889

Aurigemma, S., & Mattson, T. (2018). Exploring the effect of uncertainty avoidance on taking voluntary protective security actions. *Computers & Security*, *73*, 219–234. https://doi-org.saintleo.idm.oclc.org/10.1016/j.cose.2017.11.001

Chiasson, S., & Oorschot, P. (2015). Quantifying the security advantage of password expiration policies. *Designs, Codes & Cryptography*, *77*(2/3), 401–408. https://doi-org.saintleo.idm.oclc.org/10.1007/s10623-015-0071-9

Feldmeier, D. C., & Karn, P. R. (2001, July 6). *UNIX Password Security - Ten Years Later*. Retrieved from https://link.springer.com/chapter/10.1007/0-387-34805-0_6#citeas. doi:978-0-387-34805-6

FLORÊNCIO, D., HERLEY, C., & VAN OORSCHOT, P. C. (2016). Pushing on String: The "Don't Care" Region of Password Strength. Communications of the ACM, 59(11), 66–74. https://doi-org.saintleo.idm.oclc.org/10.1145/2934663

Guo, Y., & Zhang, Z. (2018). LPSE: Lightweight password-strength estimation for password meters. *Computers & Security*, *73*, 507–518. https://doi-org.saintleo.idm.oclc.org/10.1016/j.cose.2017.07.012

Helkala, K., & Bakås, T. H. (2014). Extended results of Norwegian password security survey. *Information Management & Computer Security*, *22*(4), 346–357. https://doi-org.saintleo.idm.oclc.org/10.1108/IMCS-10-2013-0079

Lennon, B. (2015). Passwords: Philology, Security, Authentication. *Diacritics: A Review of Contemporary Criticism*, *43*(1), 82–104. Retrieved from

https://saintleo.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=mzh&AN=2015396555&site=ehost-live&scope=site

Mayoral, F. (2013). Instant Java Password and Authentication Security : A Practical, Hands-on Guide to Securing Java Application Passwords with Hashing Techniques. Birmingham, U.K.: Packt Publishing. Retrieved from https://saintleo.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xna&AN=672977&site=ehost-live&scope=site

M c Lennan, C. T., Manning, P., & Tuft, S. E. (2017). An evaluation of the Game Changer Password System: A new approach to password security. International Journal of Human-Computer Studies, 100, 1–17. https://doi-org.saintleo.idm.oclc.org/10.1016/j.ijhcs.2016.12.003

Mishra, D. (2018). Efficient and secure two-factor dynamic ID-based password authentication scheme with provable security. Cryptologia, 42(2), 146–175. https://doi-org.saintleo.idm.oclc.org/10.1080/01611194.2017.1325787

Moshe Zviran & William J. Haga (1999) Password Security: An Empirical Study, Journal of Management Information Systems, 15:4, 161-185, DOI: 10.1080/07421222.1999.11518226

Mwagwabi, F., Mcgill, T., & Dixon, M. (2014). Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines. *2014 47th Hawaii International Conference on System Sciences*. doi:10.1109/hicss.2014.396

Purkait S, Das S. Exploring the Password Habits of Youth in Asia. IUP Journal of Information Technology. 2017;13(3):36-56.

Rass, S., & König, S. (2018). Password Security as a Game of Entropies. Entropy, 20(5), 1–12. https://doi-org.saintleo.idm.oclc.org/10.3390/e20050312

Sasse, A. (2015). Scaring and Bullying People into Security Won't Work. *IEEE Security & Privacy,13*(3), 80-83. doi:10.1109/msp.2015.65

Schoettle, A. (2018). Is your current Pa5sWoR[} strong enough? With rise of biometrics and other technology, some think it's time to change security protocol. *Indianapolis Business Journal*, *39*(24), 15A. Retrieved from https://saintleo.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bwh&AN=131199144&site=ehost-live&scope=site

Shen, C., Yu, T., Xu, H., Yang, G., & Guan, X. (2016). User practice in password security: An empirical study of real-life passwords in the wild. Computers & Security, 61, 130–141. https://doi-org.saintleo.idm.oclc.org/10.1016/j.cose.2016.05.007

Wang, D., Zhang, X., Ming, J., Chen, T., Wang, C., & Niu, W. (2018). Resetting Your Password Is Vulnerable: A Security Study of Common SMS-Based Authentication in IoT Device. Wireless Communications & Mobile Computing, 1–15. https://doi-org.saintleo.idm.oclc.org/10.1155/2018/7849065

Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: Empirical results. *IEEE Security & Privacy Magazine,2*(5), 25-31. doi:10.1109/msp.2004.81