# Effectiveness of Password Strategy

Anthony Waterman

CYSE 425W

Professor Demirel

# Effectiveness of Password Strategy

With no influence over our political, ethical, or social norms, password strategy is usually interpreted by different private and public institutions. Each institution provides general password standards. These can range from a minimum of 8 characters to a minimum of 12 characters with special symbols and numbers. Some institutions offer different fail-safes to ensure repetitive passwords are not used. Due to the lack of need for a password policy, security professionals' resort to researching new ways to secure our most used authentication option.

With a lack restrictions on password creation, most people create easy-to-remember passwords (He et al. 2019). Enforcing password enhancement during password creation would be an effective way to enhance security around an account (He et al. 2019). They suggested a two-step system in which the password would be read and if it meets all criteria, it would be accepted and the second step would be a blacklist function in which the server would check the password to see if it was on a blacklist and if this was the case, the password would be rejected (He et al. 2019). Option 2 is to introduce a hash function to encrypt the password after its entered into the system for authentication (He et al. 2019). This would reduce the burden put on the user when creating a password (He et al. 2019). The team evaluated this strategy by proposing an experiment where they used an algorithm to enhance passwords after creation. The results showed that the strategy was limited due to missed opportunities and the lack of language options for password strengthening (He et al. 2019). Because of the limited effectiveness of this strategy, there would be no policy implications. I believe an experiment using an encryption function would have seen better results due to the reduced burden on the password creator. With reduced burden and a backend encryption process, I think the demonstration would have been successful.

Another approach for password strategy was evaluated by another team. This strategy is referred to as nudging (Guo et al. 2019). The more complex the password necessary for an account, the harder it becomes to remember and that effects its usability (Guo et al. 2019). The experiment used to address this issue first proposed a dynamic personalized password policy based on personality traits (Guo et al. 2019). The experiments used DPPP which is an analysis tool that gives suggestions to the user upon password creation (Guo et al. 2019). The experiment resulted in multiple passwords being changed due to the nudge of DPPP (Guo et al. 2019). They also evaluated the password composition by performing a guessing attack. This experiment resulted in promising results but could lead to ethical implications due to the need for personality type. I believe that replacing personality types with the understanding of habits found in a work setting could have provided similar insight into cognitive ability while attempting to avoid ethical issues. I do believe the assessment I proposed would have been successful.

Another option proposed for authentication is known as recognition-based graphical passwords or RBGPs (English, 2013). An experiment was proposed to evaluate the security of this type of authentication system. The experiment used intersection attacks to try and circumvent the authentication (English, 2013). Methods 3 and 4 showed the most promise during the evaluation. The experiment concluded that adding more distractors and adjusting passimage size would reduce the successful attack percentage (English, 2013). This strategy and evaluation brought forth a lot of information and represented data. I would have assessed the strategy in the same manner and would have achieved similar results. This strategy would not lead to significant policy implications. This strategy would have to be coupled with password authentication to be considered viable.

# Works Cited

English, R. (2013). Simulating and modelling the effectiveness of graphical password intersection attacks. *Concurrency and Computation: Practice and Experience*, *27*(12), 3089–3107. https://doi.org/10.1002/cpe.3196

Guo, Y., Zhang, Z., Guo, Y., & Guo, X. (2020). Nudging personalized password policies by understanding users' personality. *Computers & Security*, *94*, 101801. https://doi.org/10.1016/j.cose.2020.101801

He, D., Yang, X., Zhou, B., Wu, Y., Cheng, Y., & Guizani, N. (2020). Password Enhancement Based on Semantic Transformation. *IEEE Network*, *34*(1), 116–121. https://doi.org/10.1109/mnet.2019.1900033