CPSC 530: Information Theory and Security
Fall 2017

Project Proposal
Estimating Password Strength

Group 3

Niroojen Thambimuthu	10153928	BSc in Computer Science
Mark De Castro	10109634	BSc in Computer Science
Minh Tran	30017773	BSc in Computer Science
Masih Sadat	10066329	BSc in Computer Science

Introduction and Problem

We are living in a digital age. Almost all parts of our lives are connected digitally to an online service: we communicate with people, we purchase things, we find entertainment—the list goes on. As such, the need to protect the sensitive information we store on these services from potential attackers have become increasingly important. Text-based passwords have become the most prominent method of authenticating ourselves into these systems and of protecting our information, despite the ever-advancing capabilities that these attackers may have.

More often than not, there are individuals who either have no knowledge of what constitutes a reliable password, or they may simply have no motivation to create a good one. It is then the responsibility of these services/websites to guide and ensure that their users are creating strong and effective passwords. They predominantly use password strength estimators (or password meters) to do so. They are usually the coloured-bars we see whenever we type in our desired password when we create an account online, and they usually indicate whether it is "strong" or "weak." However, according to Dan Wheeler's findings in his article [1], these password meters may not be as reliable as we think. For example, he found that the password "qwER43@!" is "weak" according to PayPal's password meter, while eBay's judged it as "strong." Moreover, in the research of de Carnavalet and Mannan [2], they stated that "meters from several high-profile web services (e.g., Google, Yahoo!, PayPal) are quite simplistic in nature and bear no indication of any serious efforts from these service providers." Thus, it would seem that there are inconsistencies in the policies and implementation of these websites' password meters, which may makes them look like ineffective tools of measuring actual password strength. This is an alarming precedent since it is possible for an individual to be led into believing that a password they created was "strong," when in reality, this may not be the case. This is a very concerning security risk, especially when we consider Mark Burnett's findings [3] that, while "online attacks are difficult, there are enough people with enough weak passwords that they will always yield results." Thus, ineffective password meters could mean potentially easier and/or higher number of attacks from potential hackers.

As such, having a strong and secure password has become as important as ever. With this in mind, our project therefore aims to analyze and scrutinize the efficacy of password meters deployed by a few selected popular websites. We will build upon the studies of de Carnavalet and Mannan [2], which conducted research on the practices of high-profile websites in password strength measurement. There has been a noteworthy growth in the online world ever since their studies, which include the massive growth of social media and online businesses, and thus, it would be timely to reanalyze these web services and determine how well they have kept up with their practices and policies on user password creation. We expect that our findings will help improve the password meters utilized today, and thus make them effective tools for password creation.

Proposed Work/Experiments

We have decided that we will divide the work that we will conduct on this project into two phases:

Phase One. We will study and analyze any prominent policies, characteristics and possibly algorithms (if available) of the password meters utilized by a selection of popular websites (e.g., Facebook, Twitter, Gmail, etc.). We will try to understand what policies or restrictions they impose (e.g., should passwords include a capital letter? a number?), if they perform any calculations that determine password strength (e.g., entropy), and if they employ any algorithms (e.g., to find any patterns in a password), and thus note any weaknesses or inconsistencies they may possess. We will test how these meters behave by using passwords from publicly available dictionaries. We will then compare our findings to those of de Carnavalet and Mannan [2], and note if there are any (new) significant weaknesses or inconsistencies we should highlight, and thus note any improvements that websites can implement in their password strength calculation metrics.

Phase Two. We will then utilize Wheeler's *zxcvbn* tool [1], which is a program that simulates a password meter, and we will try to make any modifications to this tool from our findings from the first phase. We will use Wheeler's tool since: (1) it is an open-source tool, and more importantly, (2) this will be a way for us to actually manipulate and tinker with a password meter (we will be using the tool that is built on Java). Hence, if we apply what we have learned from the first part of our project into this tool by trying to improve upon Wheeler's code, this may lead us into further conclusions of how password meters should or should not operate. We will do so by comparing any results we get to those of Wheeler, and if any differences arise from our modifications of his code. We will use the same data set that he utilized (Burnett's list of "Ten Million Passwords" [4]) (if it still applicable for use today; otherwise, we may have to find a more suitable/more recent set of passwords and use them for both the original and modified versions).

Therefore, the overall goal/objective of this project is to propose possible ways of improving the existing meters that these currently popular websites use. In doing so, we expect that password meters will become actual effective tools for measuring a password's strength. In turn, we expect that this will help those who may be unaware (or ignorant) of the proper techniques in formulating strong and sound passwords, which in the end, will aid in protecting their sensitive information.

Tentative Allocation of Tasks

We will divide the tasks needed to perform this project successfully as follows:

- Masih will be responsible for overseeing any programming/coding work. As this will be the most essential part of our project, the rest of the team will help him whenever necessary.
- Niroojen will handle further research work and analysis on password strength meters/estimation tools and the associated policies, algorithms and calculations that they use.
- Minh will conduct further research and analysis on what constitutes a strong password (and how they differ from weaker passwords), and thus look into the possible behavioural patterns of individuals when creating their passwords (and possibly, how attackers work as well).
- Mark will will assist Niroojen and Minh with their respective research and analysis. Additionally, he will oversee the writing of this project's technical reports.

Tentative Timeline

The group will meet every Tuesday from 9:00 to 11:00 A.M. in the CPSC Undergraduate Lab to discuss any ideas or findings we may have found about our project. A tentative timeline of what (and when) we will work on for the duration of the course is listed below:

Timeline	**Work**
Oct 7 – 25	Research on password meters used by popular websites and their efficacy
Oct 7 – 25	Compare and contrast results with the work of de Carnavalet and Mannan
Oct 7 – 25	Research on password creation patterns/techniques and their potential threats
Oct 25 – Nov 25	Study *zxcvbn* tool and modify it based on our findings and results
Nov 14 – Dec 8	Compile all findings and results for the rest of the term's deliverables
Due by Nov 26	Formulate 3 questions for Project Quiz
Due by Nov 27	Work on In-Class Presentation
Due by Nov 8	Work on Final Report

Papers/References

[1] D. Wheeler, "zxcvbn: Realistic Password Strength Estimation," April, 2012. [Online]. Available: `https://blogs.dropbox.com/tech/2012/04/zxcvbn-realistic-password-strength-estimation/`. [Accessed Oct. 1, 2017].

[2] X. de Carné de Carnavalet and M. Mannan, "From *Very Weak* to *Very Strong:* Analyzing Password-Strength Meters," presented at Network and Distributed System Security Symposium, San Diego, California, 2014.

[3] M. Burnett, *Perfect Passwords: Selection, Protection, Authentication*. Rockland, MA: Syngress Publishing, Inc., 2006.

[4] M. Burnett, "Today, I Am Releasing Ten Million Passwords," February, 2015. [Online]. Available: `https://xato.net/today-i-am-releasing-ten-million-passwords-b6278bbe7495`. [Accessed Oct. 1, 2017].