CMU CUPS Password Strength Meter

Proposal for Undergraduate Research

Seeking 9 units for the Fall 2015 semester

Henry Dixon
hdixon@cmu.edu

Faculty
Prof. Lorrie Cranor

Overview

The amount of personal information available online continues to balloon, spurring the arms race between security researchers and hackers for control of the online life. As new technologies emerge, security systems continue to evolve, with new security paradigm appearing with an increasing frequency. The password is perhaps the most fundamental and long-standing security solution found in the digital age, and relatively little has been done to improve its efficacy.

One push from the security community has been the creation and enforcement of password policies. These sterile policies are designed to improve password entropy, theoretically improving security while remaining ignorant of the user's experience. Recently, some system administrators have implemented password meters as a way to incentivize users to make more secure passwords. However, research from CMU CUPS suggests that the currently-deployed password meters are generally ineffective at improving security in a significant way. The CMU CUPS password meter seeks to improve the strength of passwords across the internet, as well as educating users on what makes a secure password.

As the opensourcemeter team is multidisciplinary, I will contribute my experience in multiple domains. I intend to use my experience with programming and data analysis to inform the design of the meter with password metrics gathered from large password dumps. Knowing about current password behavior and about attacker techniques is vital to both the design of the meter and in ensuring the safety of the recommendations it gives. I'll assist with the development of the meter using my basic knowledge of HTML, Javascript and

CSS3 – while filling in any gaps in my knowledge by further evolving my web development skillset. My parallel (although less formal) interest in design – in human interaction – is something I bring to any project. While I am not currently on track to take responsibility for major design work, I can bring an informed perspective to discussions.

State of Affairs

Previous CMU CUPS members including Maung Aung and Adam Durity have contributed a substantial codebase to the project, designing a scoring system which sequentially evaluates password rules designed to encourage stronger passwords. When I reviewed these rules alongside my analysis of a password database with experimental strength data, the connection from the rule-generated-score to the empirical strength data was not immediately apparent. Therefore, it is imperative to align the password meter's score with empirical strength data to ensure the genuine security of password-protected systems. This correction will likely involve refactoring the current codebase and considering the importance of each metric which contributes to a password's score.

Task List

1. Perform general password research to gain familiarity with the field and accepted practices
   (a) Read at least 10 research papers provided by Blase Ur
   (b) Continue research into specific password metrics to provide rules deterministic of a password's actual strength
   (c) Correlate empirical password strength with other password meters such as Dropbox's *zxcvbn* score as well as CUPS's current meter
2. Continue development of CUPS's meter
   (a) Familiarize myself with the current code base
   (b) Provide analysis of passwords to display in the interface as a means to nudge users to create stronger passwords
   (c) Refactor current code into a more testable structure
   (d) Restructure meter with rules supported by research
   (e) Implement any features requested by Blase

3. Rethink the structure of the meter's current code to provide a less arbitrary scoring system
4. Ensure the meter's recommendations are safe and correct

Grading

As the nature of the project continues to shift (e.g. we've decided to re-evaluate and rewrite much of the codebase; we have new design ideas that will inform what work needs to be done), it's difficult to provide a list of deliverables at this point in time. Checking boxes for completed tasks can be deceptive and mask some of the more subtle (yet important) aspects of research work. My reliability, ability to work with others seamlessly, willingness to take responsibility, as well as my superiors' satisfaction with the final product should all be considered.

Therefore, the project leaders (namely Blase) should assess my performance based on their overall satisfaction with my contribution to the team.