Password Strength vs Usability:
Finding Balance

David Alexander Foster | faster@ucdavis.edu
University of California, Davis | 7 June, 2017

Introduction:

The average computer user is inundated with login screens for the many accounts they access on a daily basis. The average user will have accounts for online banking, social media, message boards, corporate or educational portals, and more. According to a study conducted by Microsoft Research, the average user remembers 7 unique passwords. Many users choose passwords that are easy to remember, use a password for multiple accounts, or both, sacrificing account security for usability. For the sake of security, many online account portals have responded by requiring passwords have certain features, like a minimum character length, upper case letters, and so on. This paper explores the balance between ensuring users create passwords strong enough for the account's needs and allowing for passwords simple enough for users to easily remember.

Password Categorization:

In the paper **Guess again (and again and again)** published by researchers at Carnegie Mellon University, which we will from now on refer to simply as *Guess Again*, categories of passwords are established by length and input requirements. We adopt these categories and add a category of our own: advanced8.

The categories that will be used throughout this paper are:

- basic8 – password must have at least 8 characters
- basic16 – password must have at least 16 characters

- advanced8
    - password must have at least 8 characters
    - One uppercase letter
    - One lowercase letter
    - A symbol
    - A digit
- comprehensive8
    - password must have at least 8 characters
    - One uppercase letter
    - One lowercase letter
    - A symbol
    - A digit
    - No dictionary words

Password Requirements for Commonly used Websites:

Following is a list of commonly used websites and the password requirements for each. If possible, they are described by the aforementioned categories.

- Gmail – basic8, a dialog box warns if a password is too easy to guess
- Yahoo – 9 characters, a dialog box warns if a password is too easy to guess
- Chase Bank:
    - At least 8 characters, no longer than 32
    - At least one letter (upper or lowercase)
    - At least one number

    - At least one of these special characters: ! # $ % + / = @ ~
    - It can't include any other special characters (&, <, *, etc.)
    - It can't be the same as your username or your last 5 passwords
    - It can't include more than 2 identical letters or numbers (aaa, 111, etc.), and can't include more than 2 consecutive letters or numbers (123, abc, etc.)
- Amazon – 6 characters
- Paypal
    - At least 8 characters
    - At least one number
    - At least one symbol
    - No key sequences (like qwer or rewq)
    - No consecutive numbers
- Facebook
    - At least 6 characters
    - No key sequences (like qwer or rewq)
    - No consecutive numbers
- eBay
    - At least 6 characters
    - At least one number or symbol
    - At least 1 letter
- Linkedin
    - At least 6 characters
    - No consecutive numbers

    - No key sequences (like qwer or rewq)
- Microsoft
    - At least 8 characters
    - At least two of the following:
        - uppercase letters
        - lowercase letters
        - numbers
        - symbols
- Netflix – At least 4 characters
- Instagram
    - At least 6 characters
    - No consecutive numbers

It is interesting to note how few passwords policies examined fall under any of the categories established by researchers. Also interesting is how of the 11 policies examined, none are identical to each other; there is no standard password policy requirement shared by any of the sites examined.

User Experience for Creating Passwords:

The password requirements differ greatly from site to site, and in several instances the requirements aren't initially shown. Instagram, for example, at no point shows users what its requirements are; a red “X” simply appears in the password box until a password it deems secure enough is entered. Linkedin does not show its requirements until a password is entered that it deems insufficiently secure. Chase Bank, on the other hand, shows all of its requirements up front, of which there are **seven unique requirements**. If that were not

difficult enough, one such requirement demands users input a special character but only *certain* special characters. Creating a password with such stringent, seemingly arbitrary requirements, requires more time and patience than many users can afford. In *Guess Again*, users were asked to create passwords that follow the comprehensive8 guideline, which is similar to Chase Bank's password policy but less stringent. **Only 17.7% of participants in the study created a password that met all requirements on the first try, and 25% of participants gave up.** In fact, on average it took users on average 3.35 attempts to create a password that met comprehensive8's requirements. In a study titled **Of Passwords and People: Measuring the Effect of Password-Composition Policies**, conducted by researchers at Carnegie Mellon University and the National Institute of Standards and Technology, participants who created comprehensive8 password were asked the Likert question "Remembering the password I used for this study was difficult," to which 35% of respondents agreed, a significant difference compared to the next most difficult password, basic16, of which only 23% respondents agreed.

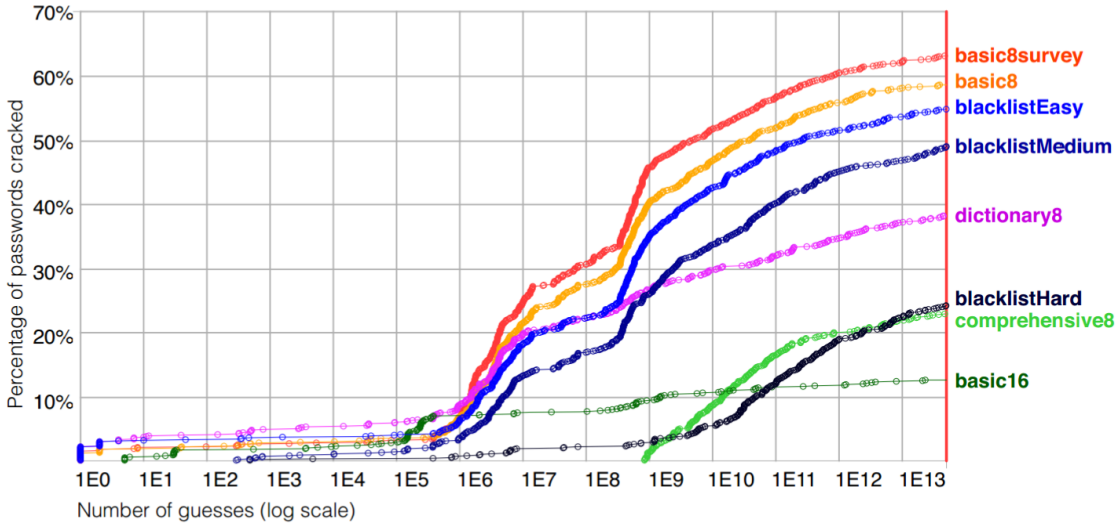
Stringent Requirements Don't Ensure Security:

One would assume the comprehensive8 password policy would be the most secure based on its stringent password requirements, but that is not the case. The basic16 password policy, in which users must enter at least 16 of any characters, is more secure. We can see from the following chart from the research paper *Guess Again* that after $1x10^{13}$ guesses basic16 passwords have a crack rate of ~14% compared to the more complex and difficult to remember comprehensive8, whose crack rate is ~23%.

Solutions:

The findings in this paper are preliminary, but a couple ideas are worth exploring further:

1. Develop universal data sensitivity based password standards for websites to adopt. For example, on websites where the compromise of a password could simply result in the impersonation of the user, a basic8 password might suffice; on websites where credit cards and other sensitive information are stored, a basic16 password may be required.



2. Develop a HTML/JavaScript Password generators plugin. Similar to Google's ReCaptcha system, which is software that acts as an anti-spam gatekeeper and is embeddable by anyone with rudimentary knowledge of HTML, an embeddable password generator could be added to account creation screens to aid users in easily creating a password secure enough for their needs.

Citations

A large-scale study of web password habits

- Microsoft Research
- http://dl.acm.org/citation.cfm?id=1242661

Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms

- Carnegie Mellon University
- http://ieeexplore.ieee.org/abstract/document/6234434/

Why your password can’t have symbols – or be longer than 16 characters

- Ars Technica
- https://arstechnica.com/security/2013/04/why-your-password-cant-have-symbols-or-be-longer-than-16-characters/

Of Passwords and People: Measuring the Effect of Password-Composition Policies

- Carnegie Mellon University, National Institute of Standards and Technology
- https://users.ece.cmu.edu/~mmazurek/papers/chi2011_passwords_people.pdf

Does My Password Go up to Eleven? The Impact of Password Meters on Password Selection

- Microsoft Research
- https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/chi13b.pdf