Study on the Password Habits of College Students

Jorge Hernandez Liang
Polytechnic University of Puerto Rico
Hernandez_89871@students.pupr.edu

Abstract

In this study we take a look at the password tendencies and habits of college students to identify strengths and weaknesses. This is accomplished by comparing given passwords by students along with their own personal demographic information with the hopes of identifying trends amongst certain groups on how they chose their passwords. From there an analysis is made to determine the presence of certain trends in some groups and if the current standards used for password requirements are adequate measures to protect these people.

Introduction

Computer security been seen as an exclusively technical field for a long time; a race between security experts trying to implement harder to break rules, more complex password policies and more taxing and complicated hashing algorithms. At its core, however, security is implemented to protect people and information that is directly or indirectly created by people. Furthermore, passwords are generally input by people, who are rarely creating a truly randomly generated password. They create these passwords in such a way that they think they can remember them, which sometimes leaves a system exposed. For this reason it is a good idea to look into not only the algorithms that are encrypting these passwords, but also the people that are creating these passwords. Even the Software Engineering Institute has since begun looking into the possibility that some things like demographic information are seriously influencing the levels of security of our passwords (CERT, 2014). Long since, the emphasis has been on creating more complex password requirements and making more complicated hashing algorithms in order to better protect our data. But why not instead of looking into these alleged sources of weakness, we look at where our strengths lie and use those to retool how to think about passwords and how to protect ourselves against possible attacks.

We analyzed a sample of college students, and asked them specific demographic information. Additionally, we requested that they answer two questions pertaining to their password habits and password generation in order to understand how this demographic deals with password security.

Background

One of the primary issues with password research and demographics is that while both individual elements are relatively accessible, finding any amount of combined data has been a challenge. For example, while there have been several leaked password sets such as the Rockyou password lists, and before that the famous Myspace leaks (Weir, M., Aggarwal, S., Collins, M., & Stern, H. ,2010), they have not come accompanied by the corresponding user's demographic information, and even then, the ethical use of that combined information without the consent of the users would have been debatable. This however was recently changed by an experiment at Carnegie Mellon University (Cranor, 2014), she discovered that passwords generated by users and collected through surveys were actually representative of the real world instances of passwords. Therefore any kind of information gained through this method can be considered valid. This can then be used as a base for future research using this method like it was done by Šolić, K., Očevčić, H., & Blažević, D. (2015) and now by ourselves. The primary difference being that this experiment was done with a broader demographic group than our own experiment. This is done with the intent to find how we can protect the people who are entering the workforce soon, even as the experts in computers. These are all people who will likely rely on passwords to keep their information secure. Being able to provide greater security to them would be of great benefit to all, both at an individual level and as organizations.

Objectives and Research Questions

Our primary goal in this research was figure out how many people, when left to determine their own requirements will continue to follow certain password complexity rules and password lengths. From there, we identified certain trends in their password habits and how each demographic fares when compared to the others. Attention was also kept upon certain recognizable patterns (Redman, 2013) that have been identified as major weaknesses in security and end up making systems more vulnerable. This is despite them being implemented in an effort to increase password complexity and safety. We identified all of the desired markers for passwords that are typically considered important for password strength. These included following the "Basic 8" rule set (minimum 8 characters), the "Complex 8 rule set" (mixed capitalizations and presence of a number or symbol), password length and compliance with the most common character pattern (first letter capitalized and the digit '1' added at the end). The users were in turn subdivided based on different demographic groups based on their answers to the first 4 questions they were given. These include dividing them by gender, age, technical background, and first language; after which the groups were identified based on what percentage of them were flagged as complying with the stated password markers. This was then repeated with combinations of these sub-groups such as for example "Spanish speaking females" to find if these subgroups were lacking or exceeding the requirements often seen by many policies.

The goal was to identify what habits can be reinforced and what habits run contrary to computer security principles. This lead us to being able to identify key strengths among some groups and this in turn could be used to implement alternate password requirements that would be more usable in practice while maintaining or possibly even increasing the security levels of our password hashes. It should also be noted that these approaches are chosen in part because they do not run contrary to other research about security and would not require a different approach to hashing and can simply be implemented alongside any other changes to password security that could be proposed.

Methods and Procedures

Data Collection

The data was gathered from 175 college students all of whom provided their answers voluntarily with no reward presented and no obligation to answer. The information provided includes various pieces of demographic information including: age range, gender, primary language, and if they work in or study in a field related to computers. They also provided a newly generated password and what they considered to be their password reuse habits. In two of the fields an option of "other (please state)" was given to allow for accuracy of answers but the totality of responses for this option is not significant enough to allow for an analysis of those demographics. The distribution of these responses is shown in Table 1.

Please note the instructions given to each person for creating our newly generated passwords. The instructions read as follows:

Please provide a password for the following fictional scenario:

"You are made aware that your email account has been compromised and are required to change the password for your personal email that is linked to your bank account log-in and social media accounts. You are told that you cannot reuse the same passwords but are given no other criteria. Please provide a newly generated password.

Note: You should not use any of your real passwords."

This was designed as such to present the respondent with a situation where the password they were generating for us represented something of value to them, be it their personal information or financial accounts. It also made it clear to them that these passwords were needed for their security, since was a system that had previously been breached in our scenario. Together, these represent a situation where the password they gave us was not simply a "throwaway" that they did not care about, there were now some stakes involved with the information they were protecting, as would be the case in many professional environments.

Table 1: Response Distribution

Question:	Response 1	Response 2	Response 3
Age:	(8) 17 or under	(53) 18 - 20	(114) 21 or Older
Gender:	(108) Male	(64) Female	(3) Other
Primary Language:	(101) English	(69) Spanish	(5) Other
Tech Related Field:	(89) Yes	(86) No	
Password Reuse:	(141) Yes	(34) No	

Results Analysis

The results were categorized based on several factors, the principal of which was the strength of the password. These were marked as complying with the "Basic 8" and "Complex 8" rule sets that were previously described. The sub divided demographic groups then were compared to each other to identify how each group naturally tended to create their passwords when not given enforced rules. The average password length and presence of the individual elements of "Complex 8" were also recorded for similar comparisons as to where the natural strengths of each group are. Results were also compared with the findings by Šolić et al. (2015) since its experiment is comparable to ours and gives us a baseline of comparing two very distinct groups, who would likely show some amount of divergence in quality of passwords and trends, if the idea that demographics do indeed influence password strength.

While most of the responses provided help for our results, some outliers were removed to preserve the integrity of the data. Specifically, those entries that are identified as not having followed the instructions. Some responses provided a template for how they would generate a password and not a password per-se. The amount of people who responded in this way was minimal but leaving them in the data set would likely lead to erroneous results. One example of this would be someone who entered as their password: "I'd change one character from the old password." and "nombredeamadaconsufechadenacimiento", which translates as "My lovers name with her birthday". Answers of this kind represented less than 3% of total answers used, so their removal is not a significant issue for this study.

Results

General Overview

Taking a general view of the results we can quickly identify the fact that the average password length is at 14.6 characters long. This is much higher than both the average of 7.8 presented in 2006 after the Myspace hack (Schneier, 2006) and the 9.6 currently stated by the Infosec Institute (Lampe, 2014). This information alone presents a significant finding since it presents us with two possibilities. Either the group as a whole is tending to passwords 5 characters longer on average or that there is a subgroup that is weighing the average to a longer length so heavily that they might require a different approach to securing their passwords to maximize their naturally created passwords. In addition, when comparing our results per demographics to those found by Šolić et al. (2015), we find our results to include less "bad" and "average" results and a greater percentage of "Good" passwords.

Subgroup Findings

When comparing certain subgroups we can begin identifying some factors that influence password length more than others. For example, the average female password in our study was found to be 13.96 characters long, this is lower than the male average of 16.68 characters, totaling a difference of 2.72 characters between them. This already marks a significant difference between some groups when making their passwords. Other broad categories did not show a significant distinction in password length. However, take for example the comparison between people who identified their primary language as English versus those who identified it as Spanish, here we see numbers of 14.68 for the former and 14.56 for the latter. A difference of a mere .12 characters, not enough to mark a need for a marked change in our analysis.

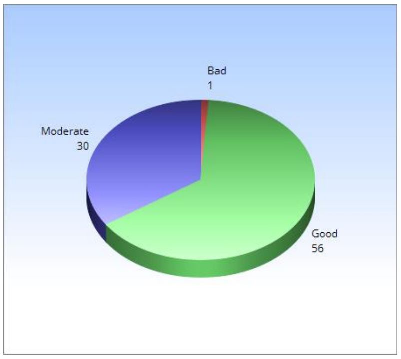
A similar split is observed for Genders when analyzing the inclusion of numbers for passwords and compliance with the “Complex 8” ruleset. As shown in Table 2, both men and women have relatively few members who fail to comply with at least the simple 8 rule set. But when a comparison is made for compliance with the complex 8 rule set we begin to see marked differences. Men as a whole tend towards the inclusion of numbers in their passwords more frequently than women. If this can be attributed to the current paradigm being more naturally favorable to the way men think or if it is simply a result of men being taught to be more aware of their passwords is outside of the scope of this study, but it is indicative of the fact that there are grounds to rethink how we currently enforce our rules if we truly wish to protect all the passwords in our system.

Table 2: Complexity divided by Gender

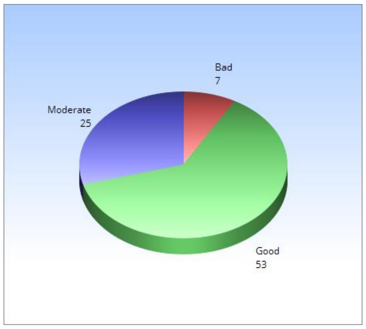
Gender	Sub 8 characters	Simple 8 Passwords	Complex 8 Passwords
Male	4(3.8%)	29(27.6%)	72(68.5%)
Female	4(6.2%)	24(37,5%)	36(56.2%)

Surprisingly one of the most unintuitive results came from dividing our samples in those that have or don't have a background in technology. As seen in Graph 1 and Graph 2 we can identify that the only significant distribution distance is a minor shift in distribution from Simple 8 passwords to Sub 8 character passwords when looking at people with a technology related background component to people without a technology related background.

What is notable however is that the sub 8 character passwords are not completely eliminated as a result and that there is comparatively little difference between the groups for Complex 8 passwords, This combined with our average password length tells us that our strong passwords tend to be quite strong by traditional metrics but our weaker passwords trail behind by a wide margin even despite the users being educated in computer knowledge. This means that there could be a significant factor outside of technical knowledge at play. This could be either a social or cultural factor. technical knowledge is not sufficient enough to make sure users are using sufficiently secure passwords.

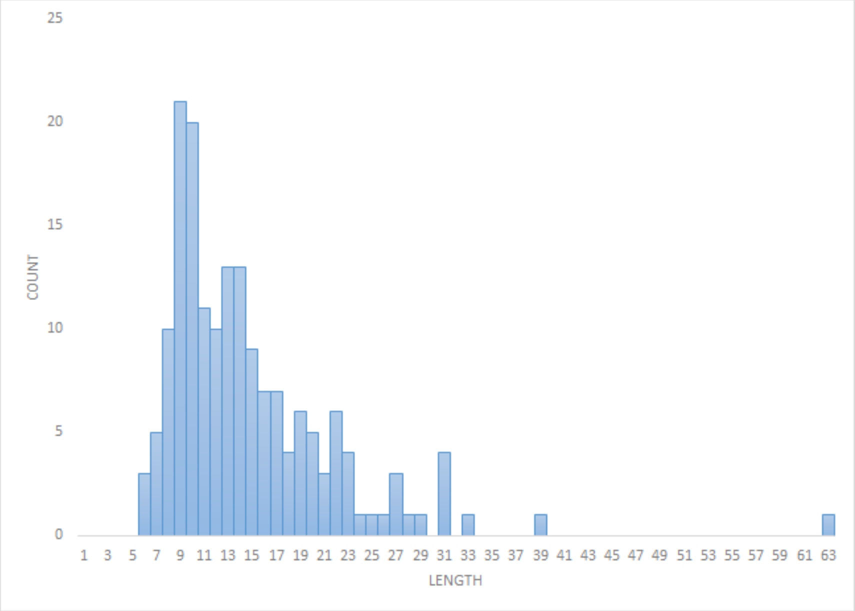


Graph 1: Users who identified as having a background in technology



Graph 2: Users who do not identify as having a background in technology

A quick glance at our password length distribution seen in Graph 3 also allows us to identify that the bulk of respondents provided passwords in the 9-10 character length range.



Graph 3: Password Length Distribution

This is another boon given that this is just barely out of the range for practical rainbow tables and rainbow table storage (List of Rainbow Tables, 2016) is already above the 650 GB range for hashed passwords of length up to 9 characters. Additionally the 10 character long passwords are only available from some groups with lowercase alphanumeric only . This temporarily places the bulk of our passwords outside of the range of attack of one of the most common methods we see today (the use of rainbow tables). Overall, we can see a strengthening of security and how our sample group is just barely winning the race against password cracking.

Conclusion

While the sample size does not allow enough room to extrapolate the resulting data, it is significant enough to prove that we are mishandling password policies at the current moment. There are several points where we can identify sub-demographics that could be much better protected by enforcing longer passwords instead of more complicated character sets. Even taking this study as an example we can clearly see a trend towards longer passwords. Instead of attempting to implement a one size fits all approach to password requirements it would be much better to have multiple “sets” of requirements and have users fulfil the criteria for at least one of them in order to accept their passwords as usable and secure. Systems are vulnerable from many angles but any intrusion could be enough to open up the entire system to an attacker, for that reason a system is only as safe as its weakest password. It should not be acceptable to continue the current trend of using these standardized methods that leave some weak individual points when they could easily be reinforced by treating them on a case-by-case basis.

It is also becoming clearer that lacking technical knowledge is not at fault for password weakness in the people we investigated. Instead of focusing our efforts exclusively on technical and general protections and measures it might be better to help defend people at an individual level. Instead how we can ease people into protecting themselves and the private systems they use instead of forcing them to conform to measures they have difficulty or simply do not care about. The current metrics are based on the rules presented in the D.o.D. Password Management guidelines book published originally in 1985. That was well before the birth of our respondents and we would be remiss without revising our ways of thinking for new users and administrators.

References

Cranor, L.F. (2014, March) Lorrie Faith Cranor: What's wrong with your Pa$$w0rd? Presented at TedxCMU 2014

List of Rainbow Tables.(n.d.).Retrieved March 11, 2016, from http://project-rainbowcrack.com/table.htm

Redman, Rick (July,2013) Cracking Corporate Passwords: Why your Password Policy Suck. Presented at Passwordcon 2013

Lampe, J. (2014, January 06). Beyond Password Length and Complexity - InfoSec Resources. Retrieved February 18, 2016, from http://resources.infosecinstitute.com/beyond-password-length-complexity/

Schneier, B. (2006, December 14). Schneier on Security. Retrieved January 11, 2016, from https://www.schneier.com/blog/archives/2006/12/ realworld_passw.html

Šolić, K., Očevčić, H., & Blažević, D. (2015). Survey on Password Quality and Confidentiality. Automatika Journal Automatika – Journal for Control, Measurement, Electronics, Computing and Communications, 56(1).

Unintentional Insider Threats: Social Engineering. (2014, January). Retrieved from https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_77459.pdf

Weir, M., Aggarwal, S., Collins, M., & Stern, H. (2010). Testing metrics for password creation policies by attacking large sets of revealed passwords. *Proceedings of the 17th ACM Conference on Computer and Communications Security - CCS '10.*