Factors Influencing Password Reuse: A Case Study

Jacob Abbott
Indiana University
jaeabbot@indiana.edu

Daniel Calarco
Indiana University
dcalarco@iu.edu

L. Jean Camp
Indiana University
ljcamp@indiana.edu

ABSTRACT

Passwords are the primary and widely used single and multiple point authentication scheme adapted across the globe. However, implemented password practices and policies varies across different platforms which creates potential security vulnerabilities. For our research, we studied the password policies of twenty-two universities and analyzed 1.3 billion email addresses and passwords obtained from Exploit.in and Anti-Public combination lists. We analyzed the potential reusability of the students, staffs, faculty, and other associated users' credentials for each of the universities' domains and checked whether they meet the specific requirements of each password policy. Through our analysis, we found several policy decisions adopted by educational institutes that may decrease security related to account credentials and make actionable recommendations for patching such security loopholes. We aim at limiting the reuse of passwords by implementing adaptive policies which will enable protection of data theft across any educational institute wide network. Our recommendations can be generalized to improve the policies adapted by several organizations in general, especially with accounts that are deemed to be highly valued, ex. email, banking, medical portal, etc.

Keywords

Passwords, Policies, Requirements, Reuse

1. INTRODUCTION

Passwords are the de facto method of authentication online, yet specific regulations and policies regarding password usage vary among different websites, platforms, and organizations. Given previous research that shows many people reuse and create weak passwords [38], this paper seeks to answer if it might be possible to reduce the likelihood of password reuse through the implementation of different password policies. Additionally, we investigated to what extent policy components may affect the likelihood of password reuse by the user by analyzing the user behaviour and practices.

To investigate the potential impact of policy on password reuse we analyzed password policies from twenty-two different U.S. universities and extracted sets of emails and passwords from two large credential data sets that were published online (Exploit.in and Anti-Public) and comprised over 1.3 billion email addresses and password combinations [43, 24]. Based on email addresses belonging to a university's domain (we checked the *.edu* domain address), passwords were compiled and tested against a university's prescribed password policy. In order to protect potential vulnerable accounts, passwords were treated as having been potentially reused if a password met all the criteria required in a university's password policy and was paired with an email matching that institution's domain address. Then it was flagged and counted as a possible reuse, otherwise it was flagged as not meeting the prescribed requirements and therefore not matching the policy of the university. Following this method, a count was established for each of the twenty-two universities regarding the number of potential pairs of reused credentials found in the leaked datasets.

In order to gauge the amount of potential password reuses and the impact of such vulnerable practices to a university's data, we requested the universities to share the actual number of active accounts that were found in the Exploit.in and Anti-Public databases. Two universities agreed to share their information with the requirement of anonymity, so we will compare the real results from the two universities with those of the twenty-two universities sampled. The aim of this detailed study and analysis is to anchor our analysis on confirmed data points to assist in providing references for the potential password reuse.

Through this analysis we find several practices which could potentially lead to future vulnerable practices and thus provide actionable recommendations on future policy usage, as authentication via applications, websites, and services continues to integrate further in everyday activities of the users. The advice of creating a unique password for every login is nearly unusuable in the past, but in today's society with the average number of password protected accounts steadily growing the task is inhuman since there is a limiataion to the memory capacity of the users [36]. We strive to suggest policies that can be used to limit the reuse of passwords with accounts that are deemed to be highly valued or of import such as, bank accounts, medical portal, emails, and other accounts.

In the following section, we begin with an overview of decades of password research and establish the requirement of such large scale comparison of password policies. We then detail the methodology in section 3 used in analyzing the data, followed by the results of the analysis in the section 4 which details the usage practices providing comparative analysis between the universities. We then move to discuss applications and implications of our research by making adaptable recommendations in section 6. We conclude by discussing about limitation of our current research in section 7 and provide concrete direction for future work in section 8.

Electronic copy available at: https://ssrn.com/abstract=3142270

2. RELATED WORK

Despite detailed work in both academic and business fields state their belief that passwords could die out and be replaced by newer authentication methods [30, 22], passwords maintain their status as the de facto authentication method employed not only through websites, but a significant number of devices as well [14]. Passwords also provide the possibility of single and multi-factor authentication system thus making them more usable and adaptable by larger user base. However, there still lies some usability issues with the current password practices of the users. Bonneau et al. reviewed multiple proposals of technologies designed to replace passwords, but found that none of the options met all requirements to address every frustration that users currently suffer from interacting with passwords [2].

Regarding passwords, the old adage of the weakest link, tends to be aimed at users and their behavior with creating and using passwords. Florencio and Herley observed half a million users and the strength of their passwords in one of the first large scale password studies finding many weak passwords [17]. Similarly, Devillers analyzed a large database of user created passwords and derived that over 90% of the passwords used were weak passwords [14] and Dell'Amico found that without enforced password policies users tend to pick weak passwords [12]. Liu et al. specifically looked at over 20 million passwords of Chinese users and found that similar to English speaking counterparts their passwords were considered weak [33]. Thus, stronger policy implementation is treated as one of the potential solutions to enhance the security practices of the users in general and reduce the possibility of using and reusing weaker passwords.

Though evidence of user behaviors' not being the most secure exists, many researchers, such as Adams and Sasse, view the supposed failing of users more as due to a failure of design rather than the fault of adversarial or apathetic users [1]. The trade-off between usability and security of authentication schemes and user behavior has been and continues to be an area of increased study [15, 16, 39, 42, 4]. Even while establishing certain policies one should be considerate about the readability and understandably of the policies for the users to understand and follow them [27, 34, 13]. Thus, implementation of passwords are not the only criteria, in fact implementation of standardized and understandable policy is preferred [40, 37].

The password polices thus developed should not only be readable, but also must be feasible and compliant with the user capabilities. Tam et al. investigated the psychology of users behind their actions [41] while Pilar tested the limitations of user's memory in using passwords [36]. Garg and Camp aimed to improve user passwords through persuasion and behavior change [19, 5]. Forget et al. tested persuasive technology to affect user behavior [18] while Yan et al. used different advice to attempt to nudge users towards better password creation habits [47]. Dell'Amico and Filiponne created a tool to check passwords to assist admins in testing their environments to potentially help them prepare for any automated attacks [11]. We must note that, keeping unique passwords for all the websites, services, and portals is not feasible and thus better tools should be developed and proper communication of the need for such password practices should be well established.

Despite continued advances in the usability and design of security tools, not all problems can be blamed or fixed through changes in user behavior. Password managers still require users to have passwords, but are aimed to reduce the stress felt by users [6, 26]. Yet even password managers cannot solve problems when websites mishandle handle passwords and expose even users who create strong passwords through technical failures outside their control [3].

A growing number of sites promote the use of multi-factor authentication tools to remove passwords as a single fail point for accessing accounts, yet most implementations suffer from their own issues with usability and still require the use of passwords as one factor regardless of if they use biometrics [35], one time codes [10, 21, 46], or hardware tokens [20, 32, 45, 9].

The threat of password reuse is still impactful as two-factor authentication is not mandatory everywhere and does not completely remove dangers presented by password reuse [8, 25]. Our investigation thus provides an insightful discussion on how after decades of research on the password usage behavior, users are still reusing passwords and also how design modifications, risk communication, and policy modifications combined together can help in creating a secure environment.

Big 10	Western Universities
Ohio State U.	U. of California Davis
Michigan State U.	U. of California Los Angeles
Indiana U.	U. of Washington
Purdue U.	Loyola Marymount University
U. of Michigan	Pomona College
U. of Illinois	Pepperdine University
U. of Iowa	U. of California Berkeley
U. of Nebraska	U. of Southern California
U. of Maryland	U. of California San Diego
Rutgers U.	Claremont McKenna College
Northwestern U.	
U. of Minnesota	

Table 1: Universities originally selected for analysis

3. METHOD

Policies from the "Big 10" universities in the United States that are located in the eastern half of the country were selected for analysis after a report identified millions of university email credentials were for sale on the Dark Web [23]. Additionally a similar number of universities from the western half of the United States were selected to increase the sample size for investigation. Password policies and account creation details were collected for each of the selected universities and the text was analyzed to measure the readability of the password policies using the Flesch-Kincaid readability score metric. The Flesch reading and Flesch-Kincaid readibility scores were chosen as they have been used as reliable readability metrics for decades and serve as a point of reference [28].

To investigate if password policies have an effect on potential password reuse, email addresses ending with ".edu" and their corresponding passwords were pulled from the Exploit.in and Anti-Public combo lists as described by Hunt's article that described the two datasets comprising over 1 billion credential records [24]. Of the 1.3 billion records, 7,384,281 were associated with a ".edu" address. From the full set of university related emails a subset was pulled out to match each of the specific university's domain. Table 1 shows the full list of universities analyzed.

In order to maintain security of accounts and handle the data ethically, researchers did not actually test if emails and passwords were active at different university's. Instead each subset of data was tested against the university's published password policies to test if the password listed in the datasets could meet the requirements listed and therefore theoretically be a potentially reused password.

Electronic copy available at: https://ssrn.com/abstract=3142270

University password policies were also measured on the minimum length required by their passwords as well as the stated required complexity of the policies. Policies were considered to have higher complexity requirements based on the number of different character types that were specifically required between lowercase alphas, uppercase alphas, numbers, and special characters.

Further policy information was recorded for each of the policies when expressed, but not all universities specified the same criteria. The additional information recorded included the maximum length of passwords allowed, whether password duration was listed, how long a password could be used before expiration, whether reuse of previous passwords was prohibited, and if prohibited how far into the past passwords were checked against for reuse. Some additional notes that did not fit into specific trends were observed across multiple universities and were recorded on an individual basis.

4. FINDINGS

Here we describe the factors of passport practices obtained from our investigation. We also note the readability and literacy requirements of the password policies for the different universities and the rate of credentials from Exploit.in and Anti-Public datasets matching the individual password policy requirements. We provide detailed information of the mismatch between the password policies implemented across different universities, as well as what is shared across the different policies.

4.1 Policy Readability

Of the twenty-two universities originally selected to have their password policy analyzed, researchers were unable to obtain a password policy for Claremont McKenna College that was accessible to the public, therefore they are omitted from the analysis with the twenty-one additional universities still being reported. The first task after collecting password policies was to gather the Flesch Reading score to measure readability and the Flesch-Kincaid score for the grade literacy required to understand the text. Figure 1 shows the Flesch Reading score for each of the university password policies. The higher the Flesch Reading score, the easier a document is considered to read and understand. For example a score of 90 or higher is considered to be very easy to read, with 80 to 89 being easy, 70 to 79 is fairly easy, 60 to 69 as standard difficulty, and 50 to 59 as being fairly difficult. A score between 30 and 49 is considered difficult and anything below 30 is considered very difficult and confusing.

As evidenced in Figure 1 the four highest scored password policies fell into the standard difficulty rating with Pomona College scoring the highest at 62.9. Eight other universities fell into the fairly difficult category. The remainder of the password policies were rated as being difficult to read and comprehend, with the exclusion of University of Iowa's policy which was the only score observed to fall into the very difficult category with a score of 24.

Table 2 shows the Flesch-Kincaid [17] score for grade level literacy required for each of the password policy documents. The median of all twenty-one universities scored a 10 indicating a U.S. tenth grade reading level as being appropriate to understand the policy document. The lowest grade score was observed by Pomona College's policy that suggested a sixth grade reading level. The highest observed was that of University of Iowa which scored a 14, which would roughly be a second year undergraduate student reading level. The majority of policies fell between requiring a ninth or eleventh grade reading level.

4.2 Password Policy Matches

Big 10	Score	Western Universities	Score
Ohio State U.	8	U. of California Davis	9
Michigan State U.	8	U. of California Los Angeles	9
Indiana U.	11	U. of Washington	11
Purdue U.	12	Loyola Marymount University	11
U. of Michigan	8	Pomona College	6
U. of Illinois	7	Pepperdine University	9
U. of Iowa	14	U. of California Berkeley	10
U. of Nebraska	10	U. of Southern California	10
U. of Maryland	11	U. of California San Diego	11
Rutgers U.	10		
Northwestern U.	11		
U. of Minnesota	11		

Table 2: Flesch-Kincaid Grade Level Score by University

From the 1.3 billion credentials found in the Exploit.in and Anti-Public datasets there were nearly 7.4 million email addresses associated with .edu domains. Of those 7.4 million addresses the twenty-one universities analyzed here made up 533,927 observations from the datasets. Table 3 shows a breakdown of the number of email addresses observed from each university in the datasets. The results include repeated email addresses that were paired with different passwords in the datasets. Each password was tested against the password policy of the corresponding university and was counted as a potential reuse if the password matched the requirements as listed in the policy document regarding both length and complexity requirements. The number of observed policy matches and the rate for each university is listed in Table 3. The frequency of potential reuse based on matching university policy requirements ranged from almost zero with Indiana University (0.02%), University of Iowa (0.17%), and University of California Davis (0.26%) all having less than 1% observed as being potentially reused university credentials all the way up to essentially a coin toss as seen with University of California Los Angeles (45.03%), University of Washington (51.68%), and University of California San Diego (56.79%). Again these numbers do not reflect actual password reuse, but merely the potential of university credential reuse given the password and email address in the published datasets.

Such large differences in the likelihood of potential reuse across different universities with a number of unique policies led to the researchers looking for similarities and differences between policies. To that end university policies were grouped into categories based on their minimum password length to explore potential impact of minimum length requirements.

4.3 Minimum Password Length Requirements

Figure 2 shows each university's minimum required length for passwords according to their published policy. Thirteen of the twenty-one universities required a minimum of 8 characters for passwords, while two universities had a minimum requirement of 7 characters. Two universities required 9 characters, while an additional three universities had a minimum of 12 characters. Only Indiana University required more than 12 characters for passwords

Electronic copy available at: https://ssrn.com/abstract=3142270

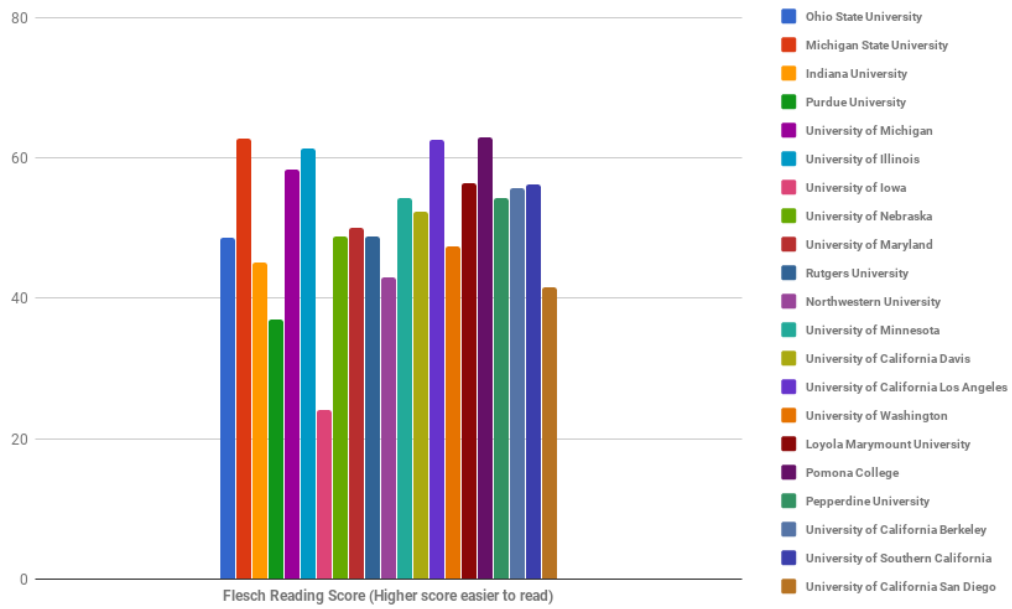

Figure 1: Flesch Reading Score by University

Big 10	Addr.	Policy Matches
Ohio State U.	52,299	2,171 (4.15%)
Michigan State U.	66,120	6,356 (9.61%)
Indiana U.	71,096	15 (0.02%)
Purdue U.	38,441	2,550 (6.63%)
U. of Michigan	56,510	15,073 (26.67%)
U. of Illinois	8,871	2,518 (28.38%)
U. of Iowa	19,574	34 (0.17%)
U. of Nebraska	3,721	100 (2.69%)
U. of Maryland	2,231	293 (13.13%)
Rutgers U.	3,763	281 (7.47%)
Northwestern U.	13,020	1,028 (7.90%)
U. of Minnesota	41,322	5028 (12.17%)
Western Universities	**Addr.**	**Policy Matches**
U. of California Davis	23,855	62 (0.26%)
U. of California Los Angeles	25,770	11,603 (45.03%)
U. of Washington	29,999	15,503 (51.68%)
Loyola Marymount University	779	74 (9.50%)
Pomona College	2,051	343 (16.72%)
Pepperdine University	5,470	344 (6.29%)
U. of California Berkeley	20,425	1,293 (6.33%)
U. of Southern California	28,868	862 (2.99%)
U. of California San Diego	18,831	10,694 (56.79%)

Table 3: Number of emails by university in dataset and potential password reuse rates.

Minimum Length	University	Policy Matches
Min 7	U. Michigan, UC San Diego	34.2%
Min 8	Ohio State, Michigan State, Purdue, Illinois, Nebraska, Maryland, Rutgers, Northwestern, Minnesota, UC Los Angeles, Washington, Loyola, Pomona	16.59%
Min 9	Iowa, UC Berkeley	3.32%
Min 12	UC Davis, Pepperdine, U. of Southern California	2.18%
Min 15	Indiana	0.02%

Table 4: Universities grouped by minimum password length requirement

to meet the minimum requirement of 15 characters. Table 4 shows the universities grouped by their minimum length and the likelihood of password reuse of that group combined. There is a distinct trend of having a higher minimum length required reducing the likelihood of reuse across multiple universities.

4.4 Password Complexity Requirements

Figure 3 shows the complexity requirement by each university's policy. The policy's complexity requirement is rated based on the number of distinct character types that are mentioned as being re-

Electronic copy available at: https://ssrn.com/abstract=3142270

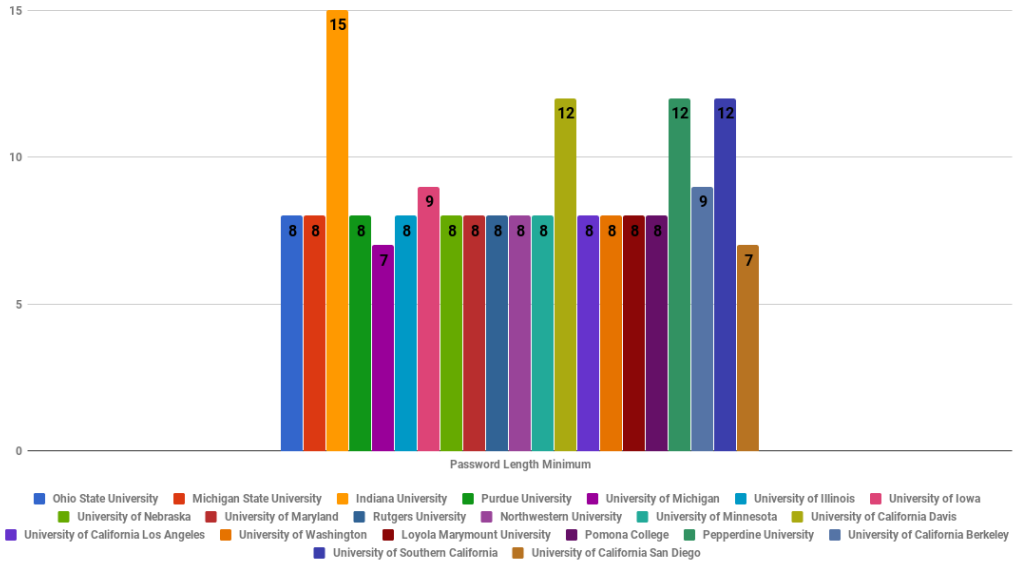

Figure 2: Minimum Password Length Required by University

Requirements	University	Policy Matches
1 Req	Northwestern, U. of Southern California	4.51%
2 Req	Purdue, UC Los Angeles	22.04%
3 Req	Ohio State, Michigan State, U. of Michigan, Illinois, Nebraska, Maryland, Rutgers, Minnesota, Washington, Loyola, Pomona, Pepperdine, UC Berkeley, UC San Diego	19.12%
4 Req	Indiana, Iowa, UC Davis	0.10%

Table 5: Universities grouped by number of character types required

quired. For example, a policy requiring at least one lowercase alpha, uppercase alpha, number, and special character would receive a complexity rating of 4, while a policy that specifically only requires an alpha and digit would receive a complexity rating of 2. Despite not specifying requirement of higher complexity, it should be noted that none of the observed university's forbade passwords of higher complexity than the required limit, excluding some specific symbols that could not be used.

Table 5 shows the universities grouped by their complexity requirement along with the likelihood of reuse by each group. Only two universities fell into the complexity rating 1 category, two in complexity rating 2, and three in complexity rating 4. Fourteen of the twenty-one universities fell into the complexity rating 3 category. Similar to length, there is a distinct trend towards higher complexity having a lower likelihood of being reused.

4.5 Additional Requirements

Beyond the investigation into length and complexity requirements in university password policy, additional information was presented in certain policies. Eleven of the twenty-one universities reported specific maximums for their password length. Two universities maxed their password length at 16 characters, while others spread out all the way to University of California Berkeley's maximum of 255 characters. Of the observed universities the vast majority of passwords were never close to reaching the maximum requirements of any of the universities. Regarding the Big 10 and the Western Universities, both sets matched in their password lengths from medians at 8 characters up to 90% quantile of 10 characters in length. The observed credentials for Big 10 universities hit 12 characters in length at the 95% quantile while the Western universities were up to 15 characters at the 95% quantile. We can infer that even the lowest maximum wasn't met by at least 95% of the observed passwords.

Thirteen of the twenty-one universities also published the maximum duration passwords could be used before expiration ranging from a minimum of six months all the way up to two years. Similarly nine of the twenty-one universities specifically forbade reuse of previous passwords, though only four gave a specified number of previous passwords that would be checked against.

Furthermore ten of the universities had policies that featured additional notes or requirements that did not fall into previous categories. For example the University of California Berkeley specifically stated that passwords must pass a CrackLib test to be allowed. Two universities specified that the password could not include the user's name or username. University of Washington was the only university to specifically identify the number of failed authentication attempts before account lockout.

5. DISCUSSION

Reuse of passwords is not ideal in the sense of security, but it happens frequently enough that it is often considered common place, as very few people can truly claim to use a unique password for every site or account they have. Many users may cite ease of use or similarity between sites as reasons for reusing credentials, but the risk of reusing credentials from a university account are

Electronic copy available at: https://ssrn.com/abstract=3142270

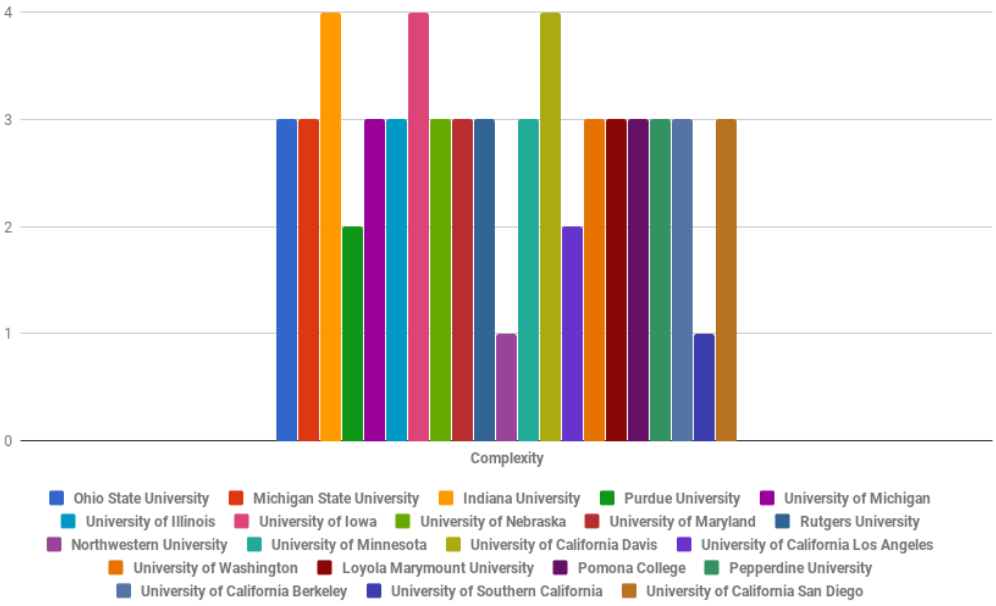

Figure 3: Password Complexity by University

not insignificant. Krebs' article on the value of a hacked email account can easily be juxtaposed to a university account [31]. Many students work while attending university and if they are employed by their respective university it is likely they have personal financial information connected to their university credentials, as well as tax records, calendar information, personal communications, and more. Therefore, credential reuse can pose a significant risk if users are not cautious or if their data is mishandled.

The danger is not only posed to affect students but also staff and faculty of universities who may reuse their credentials. The threat of faculty and staff having credentials reused may pose a greater threat as faculty and staff are more likely to have access to more information and permissions than students.

The majority of university password policies' Flesch-Kincaid school grade score fell in the mid-high school level for the literacy rate required to comprehend the policy. The majority of policies fell into the difficult and somewhat difficult to read categories for their Flesch readability score. The requirement of high school literacy may be seen as an acceptable level for those affiliated with the university, but it remains to be seen if a lower literacy requirement would have a significant increase in the usability of passwords.

The potential reuse of passwords that match the published university policies does not accurately predict the actual rate of password reuse. As previously mentioned two universities shared their own findings from checking the Exploit.in and Anti-Public databases for potentially vulnerable accounts. The average result from the two universities showed a likelihood of 1.5% of an account being active and the credentials being reused. Despite 1.5% being significantly lower than a number of the potential reuse rates identified through simply checking against the minimum length and complexity requirements, that could still be a significantly large number of accounts. If we take the 1.5% as a baseline, then of the 7,384,281 accounts associated with .edu addresses a total of 110,764 would be actively vulnerable from the reused credentials.

The thought experiment regarding the number of vulnerable accounts cannot be confirmed, but we could additionally push this thought out to other accounts of import, such as banking sites. Overtime research has shown that people continue to create better password and that changes to policies can affect behaviors [29], but many users are creating better passwords because of adjustments to policies, such as increases the minimum length from 6 to 8 characters. The trend of higher minimum length requirements having lower likelihood of reuse might be due to the tendency of people to meet the minimum requirements of policies.

Similarly the increase in password complexity showed a trend towards a decrease in the likelihood of credential reuse, but attempting to increase the complexity requirements of passwords may be implausible. What additional characteristics could be required of a policy that already requires the use of lowercase alphas, uppercase alphas, digits, and symbols to increase the complexity is an open question that is open for future work.

Additional information regarding password policies such as the duration before expiration, the number of attempts before a lockout, or forbidding certain password constructions may benefit the universities. However, due to the low number observances no strong points could be observed regarding these points. Further investigation into these factors may lead to additional insights in the future.

6. RECOMMENDATIONS

Some changes to policies may have greater effects on reducing risk to an organization than others, but there are different costs in usability or actual financial cost, such as implementing multi-factor authentication, when implementing changes in policies. The following recommendations are based on previous literature and observations of this paper.

1. **Increase the minimum password length beyond 8 characters.**

   An increase to the minimum length required for passwords would put the new minimum higher than over 50% of the observed passwords in the entire set of .edu addresses present

Electronic copy available at: https://ssrn.com/abstract=3142270

in the Exploit.in and Anti-Public datasets. With the trend of users to meet the minimum requirements, having a higher minimum requirement for high value sites and accounts could potentially lead to reduced likelihood of credential reuse for lower valued accounts with lower minimum requirements.

2. **Increase maximum password length.**

   The recommendation to increase the maximum length allowed for passwords should be done so selectively. Increasing the maximum over the minimum of other policies will allow for a wider range of choices for users. Having a maximum of 12 characters, for example, may increase the likelihood of password reuse on other sites that also contain a low ceiling on the max length of their passwords.

3. **Disallow the user's name or username inside passwords.**

   Removing the ability of users to include their name or username inside passwords will additionally remove the ability to have the password and username match. This simple distinction may reduce the likelihood of credential reuse as it may increase the difficulty of guessing the account's password.

4. **Contemplate multi-factor authentication.**

   Multi-factor authentication is becoming more common and usable [7, 44]. With potential benefits of reducing the risk of password reuse, multi-factor authentication may be a viable option to replace changes to the length and/or complexity of password policies.

7. LIMITATIONS

The Exploit.in and Anti-Public databases available are from a number of previous breaches and leaks that were compiled together with the articles announcing the datasets in the spring of 2017. Therefore, there are a number of credentials that might not meet the requirements for duration even if they were actually reused. Because we cannot tell when credentials were taken and will not test the validity of credentials on any university's system, we can only report on credentials that meet the policy requirements of minimum password length and password complexity.

Additionally, given the nature of the datasets we cannot be certain that credentials are or ever were real, it is possible that credentials were fabricated, both email addresses and passwords. Due to ethical concerns we made no effort to test the validity of email and password pairs and only tested passwords against the published password policies of each university.

There still exists the potential of users' passwords being reused with an email address not associated with a university. This potential is outside the scope of the project and was not considered when processing the data and looking at the potential password reuse of the university credentials.

8. FUTURE WORK

Additional research can be targeted towards how to increase the complexity of passwords beyond requiring four different character types. This can be done by requiring passphrases using spaces or potentially by disallowing certain combinations of characters, such as sequential numbers or characters closely located on a keyboard (ex. "QWER"). We can also change the frequency of password expiration or the number of login attempts before lockout. To what extent potential changes this would have on security and user behavior is an open question. Certain techniques are implemented in banking sectors and could be implemented to protect important and confidential data for universities.

Websites that provide email addresses like Gmail or Yahoo may be ripe for additional examination comparing their password policies using the same methodology as that employed to test the .edu addresses from the Exploit.in and Anti-Public datasets. Finding and examining the policies of non-educational organizations may highlight distinct differences in organizational behavior regarding security policies.

Given the large amount of data contained in the Exploit.in and Anti-Public datasets with over 1.3 billion email addresses and passwords, exploration of unique accounts may yield some larger insights into the password creation and usage patterns. Despite the large number of .edu domain addresses it only comprised 0.057% of the full dataset. With observations of this, relatively, small sample, the exploration of potential password usage difference across domains with specific geographic codes, such as .de for Germany or .fr for France, may provide unique insights into individual countries as well as potentially global trends that may exist despite geographical, cultural, or linguistic differences.

9. CONCLUSIONS

Passwords continue to be a necessity in the daily lives of millions around the world, yet the collective wisdom still maintains that passwords are difficult to use and the best security practices are not humanly possible. Yet this investigation looked into how policies might effect user behavior in reusing credentials from a high valued account and our method identified policy matches as potential reuse since calculating true reuse of credentials posed significant ethical complications.

We found that requiring longer and more complicated passwords trended towards a lower likelihood of password reuse. Additionally, we found that the majority of password policies were difficult to very difficult to read and understand according to the Flesch reading scale and typically have a literacy requirement of high school level.

We give recommendations for potential policy changes that might further reduce the likelihood of credential reuse without impacting the feasibility of implementing such password practices. Our recommendations are not only applicable for universities, but also can be used by other organizations , services, or applications, with high value accounts and point to areas of interest for future work.

10. ACKNOWLEDGMENTS

This research was supported in part by the National Science Foundation under CNS 1565375, Cisco Research Support, and the Comcast Innovation Fund. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the the US Government, the National Science Foundation, Cisco, Comcast, nor Indiana University. Additional thanks to Sanchari Das and Chamikara Arachchige for their insights.

11. REFERENCES

[1] A. Adams and M. A. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[2] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. Technical report, University of Cambridge, Computer Laboratory, 2012.

[3] J. Bonneau and S. Preibusch. The password thicket: Technical and market failures in human authentication on the web. In *WEIS*, 2010.

[4] C. Braz and J.-M. Robert. Security and usability: the case of the user authentication methods. In *Proceedings of the 18th*

Electronic copy available at: https://ssrn.com/abstract=3142270

Conference on l'Interaction Homme-Machine, pages 199–203. ACM, 2006.

[5] L. J. Camp, J. Abbott, and S. Chen. Cpasswords: Leveraging episodic memory and human-centered design for better authentication. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pages 3656–3665. IEEE, 2016.

[6] S. Chiasson, P. C. van Oorschot, and R. Biddle. A usability study and critique of two password managers. In *USENIX Security Symposium*, pages 1–16, 2006.

[7] J. Colnago, S. Devlin, M. Oates, C. Swoopes, L. Bauer, L. Cranor, and N. Christin. âĂIJit's not actually that horribleâĂİ: Exploring adoption of two-factor authentication at a university. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, page 456. ACM, 2018.

[8] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang. The tangled web of password reuse. In *NDSS*, volume 14, pages 23–26, 2014.

[9] S. Das, A. Dingman, and L. J. Camp. Why johnny doesnâĂŹt use two factor a two-phase usability study of the fido u2f security key. In *2018 International Conference on Financial Cryptography and Data Security (FC)*, 2018.

[10] E. De Cristofaro, H. Du, J. Freudiger, and G. Norcie. A comparative usability study of two-factor authentication. *arXiv preprint arXiv:1309.5344*, 2013.

[11] M. Dell'Amico and M. Filippone. Monte carlo strength evaluation: Fast and reliable password checking. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 158–169. ACM, 2015.

[12] M. Dell'Amico, P. Michiardi, and Y. Roudier. Password strength: An empirical analysis. In *INFOCOM, 2010 Proceedings IEEE*, pages 1–9. IEEE, 2010.

[13] J. Dev, S. Das, and K. Srinivasan. Modularity is the key: A new approach to social media privacy policies.

[14] M. M. Devillers. Analyzing password strength. *Radboud University Nijmegen, Tech. Rep*, 2, 2010.

[15] P. Dourish, E. Grinter, J. Delgado De La Flor, and M. Joseph. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6):391–401, 2004.

[16] B. Fischhoff, P. Slovic, S. Lichtenstein, S. Read, and B. Combs. How safe is safe enough? a psychometric study of attitudes towards technological risks and benefits. *Policy sciences*, 9(2):127–152, 1978.

[17] D. Florencio and C. Herley. A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web*, pages 657–666. ACM, 2007.

[18] A. Forget, S. Chiasson, P. C. van Oorschot, and R. Biddle. Improving text passwords through persuasion. In *Proceedings of the 4th symposium on Usable privacy and security*, pages 1–12. ACM, 2008.

[19] V. Garg and L. J. Camp. Heuristics and biases: Implications for security. *IEEE Technology & Society*, 2013.

[20] E. Grosse and M. Upadhyay. Authentication at scale. *IEEE Security & Privacy*, 11(1):15–22, 2013.

[21] N. Gunson, D. Marshall, H. Morton, and M. Jack. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security*, 30(4):208–220, 2011.

[22] C. Herley, P. C. van Oorschot, and A. S. Patrick. Passwords: If weâĂŹre so smart, why are we still using them? In *International Conference on Financial Cryptography and Data Security*, pages 230–237. Springer, 2009.

[23] K. J. Higgins. Millions of stolen us university email credentials for sale on the dark web, Mar 2017.

[24] T. Hunt. Password reuse, credential stuffing and another billion records in have i been pwned, Dec 2017.

[25] B. Ives, K. R. Walsh, and H. Schneider. The domino effect of password reuse. *Communications of the ACM*, 47(4):75–78, 2004.

[26] A. Karole, N. Saxena, and N. Christin. A comparative usability evaluation of traditional password managers. In *International Conference on Information Security and Cryptology*, pages 233–251. Springer, 2010.

[27] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder. A nutrition label for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, page 4. ACM, 2009.

[28] J. P. Kincaid, R. P. Fishburne Jr, R. L. Rogers, and B. S. Chissom. Derivation of new readability formulas (automated readability index, fog count and flesch reading ease formula) for navy enlisted personnel. 1975.

[29] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman. Of passwords and people: measuring the effect of password-composition policies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2595–2604. ACM, 2011.

[30] M. Kotadia. Gates predicts death of the password, Feb 2004.

[31] B. Krebs. Krebs on security, Jun 2013.

[32] K. Krol, E. Philippou, E. De Cristofaro, and M. A. Sasse. "they brought in the horrible key ring thing!" analysing the usability of two-factor authentication in uk online banking. *arXiv preprint arXiv:1501.04434*, 2015.

[33] Z. Liu, Y. Hong, and D. Pi. A large-scale study of web password habits of chinese network users. *JSW*, 9(2):293–297, 2014.

[34] A. M. Mcdonald, R. W. Reeder, P. G. Kelley, and L. F. Cranor. A comparative study of online privacy policies and formats. In *International Symposium on Privacy Enhancing Technologies Symposium*, pages 37–55. Springer, 2009.

[35] L. O'Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12):2021–2040, 2003.

[36] D. R. Pilar, A. Jaeger, C. F. Gomes, and L. M. Stein. Passwords usage and human memory limitations: A survey across age and educational background. *PloS one*, 7(12):e51067, 2012.

[37] A. Raikar and G. Ramarao. Method and system for establishing a consistent password policy, Dec. 7 2010. US Patent 7,849,320.

[38] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor. Encountering stronger password requirements: user attitudes and behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, page 2. ACM, 2010.

[39] E. Stobert and R. Biddle. The password life cycle: user behaviour in managing passwords. In *Proc. SOUPS*, 2014.

[40] W. C. Summers and E. Bosworth. Password policy: the good, the bad, and the ugly. In *Proceedings of the winter international synposium on Information and communication technologies*, pages 1–6. Trinity College Dublin, 2004.

Electronic copy available at: https://ssrn.com/abstract=3142270

[41] L. Tam, M. Glassman, and M. Vandenwauver. The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, 29(3):233–244, 2010.

[42] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor. I added âĂŸ!âĂŹat the end to make it secureâĂİ: Observing password creation in the lab. In *Proc. SOUPS*, 2015.

[43] D. Walker. Breach site finds 1 billion accounts in hacked datasets, May 2017.

[44] J. Weidman and J. Grossklags. I like it, but i hate it: Employee perceptions towards an institutional transition to byod second-factor authentication. In *Proceedings of the 33rd Annual Computer Security Applications Conference*. ACM, 2017.

[45] C. S. Weir, G. Douglas, M. Carruthers, and M. Jack. User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security*, 28(1-2):47–62, 2009.

[46] M. Wu, S. Garfinkel, and R. Miller. Secure web authentication with mobile phones. In *DIMACS workshop on usable privacy and security software*, volume 2010, 2004.

[47] J. Yan, A. Blackwell, R. Anderson, and A. Grant. Password memorability and security: Empirical results. *IEEE Security & privacy*, 2(5):25–31, 2004.

Electronic copy available at: https://ssrn.com/abstract=3142270