Analysis of Coping Mechanisms of Password Selection

Brian Curnett, Paul Duselis, and Teri Flory

INSURE Program, Purdue University

April 25, 2014
Abstract

There have been multiple previous studies on password entropy and attacks on passwords. However, there is currently a lack of research available on the effect of required regular password modifications, and whether those requirements lead to users reverting to coping mechanisms. Further, there has been limited work on the effects of users reverting to coping mechanisms when confronted with password policies that are cumbersome and stringent.

Among the computer science field, passwords are often reviewed using the concept of entropy as a means to measure the strength of a password against a brute force attack. Many policies focus on increasing the entropy of the password to the detriment of the user. By recognizing the limits of the user’s memory, policies can be created that do not frustrate, confound, and anger the user. Coping mechanisms may include users writing passwords down, incrementing passwords over time, or sharing a password across multiple accounts. By acknowledging these tendencies, password policies can be crafted that mitigate these coping mechanisms, and allow for true protection of accounts on both an entropy based level and the human element. The survey formulations and assessments will be described to study these password coping mechanisms. Further, this data can serve as an useful input for exploring the alternatives to password authentication, such as the adoption of biometric options, Smart Cards, Radio-Frequency Identification, hardware tokens, or other non-password security measures.

Keywords: coping mechanism, entropy, password, password analysis, password frustration, password policies, password strength, risk analysis, strength analysis, user behavior
Analysis of Coping Mechanisms of Password Selection

Motivation

Stringent password policies can cause users to adopt coping methods that undermine the policy’s effectiveness. Passwords are required as an authentication mechanism for many daily tasks throughout society, including financial transactions, shopping, communication, and work. The challenge is to determine at what point a password policy is undermined by human nature, and to consider that threshold when creating or modifying current policies.

Many users understand security needs, but the policies imposed to meet those needs are often cumbersome, and lead to the use of coping mechanisms. These include writing down passwords, utilizing the same password across multiple accounts, doubling the password, slightly modifying the password by incrementing the number or special character, or even forgetting the password, requiring a reset which often takes time and decreases productivity.

This work proposes a method of data collection and an analysis of the data that is collected in order to test our hypothesis, which we anticipate will show users reverting to coping mechanisms when they are required to create passwords. There will be three separate password policies utilized to observe whether there is a distinction between the policy requirements and the likelihood that users will resort to coping mechanisms.

Previous Work

Coping Mechanisms. Common password policies in effect at organizations and corporations range from Basic8, which only requires eight characters, to Comprehensive24, which requires twenty-four characters, and includes a capitalized letter, lower-case letter, number, and special character. Policies are now also requiring users to refrain from a word that can be found in a dictionary. Throughout the preparation of this work, the researchers were also
told anecdotal stories from interested parties regarding password policies in effect at his or her place of employment, passwords written down on small notes throughout an individual’s office, and of a password reset, which took three hours of the employee’s time before he was able to log back into the system. The issue of password policies, and specifically coping mechanisms, affects a large percentage of the population, and can have far reaching and damaging consequences if the data protected by passwords is not kept safe.

According to Inglesant and Sasse (2010), due to the stringent password policies that are now in place at many organizations, users often choose the weakest password they are allowed under these policies. They were interested in how password experiences affect users, and as an extension, an organization’s productivity, and they reviewed both the users complicity with the password policy, but also the way the policy positively or negatively impacted the users’, and therefore, the organizations’ productivity. The study followed a small group of individuals (thirty-two individuals) employed at two separate organizations, each with a different policy, for approximately one week. The participants kept journals of password events throughout the week and also took part in video journals at the end of the study. Researchers specifically found that users understand security needs but that they perceived password policy demands as too difficult, that users cope with the policy requirement of changing passwords by writing them down, and that the security policy of the organization needs to be written to balance the security needs with the capabilities of the users. The researchers utilized this study as a starting point for our data collection method, as the journal provides for the historical changes in passwords, and how this affects users transitioning to coping methods. Further, the authors found that the organization with a stricter password policy on utilizing previous password variations had a much greater number of users writing down the passwords. Our data collection method will be different in that
we aim to provide a much greater number of participants, which will provide a more quantitative analysis. However, it is noted that the Inglesant and Sasse (2010) study followed employees and reviewed passwords in a real world setting, whereas our study will utilize students at a university with a fictional password.

Password policies often require individuals to try and retain random sequences of numbers, letters, and symbols, or often require individuals to change or modify his or her password periodically. This issue is further complicated if the individual is not allowed to reuse all or parts of a password that has been utilized in the past. According to Komanduri et al. (2011), their short term password recall and creation study found these policies often lead to individuals writing down passwords, and found that after two days, 31% of 3,056 participants recorded passwords either electronically or on paper. Komanduri, Shay, Kelley, Mazurek, Bauer, Cristin, Cranor, and Egelman (2011) also found that users would fall into two categories when creating a password for a specific policy. The first category consisted of those who would incrementally modify a password until it fit the policy while the second group consisted of those who would change their password to something entirely different. Long term recall was reviewed by Zhang, Luo, Akkaladevi, and Ziegelmayer (2009), as well as the added complication of many users having multiple passwords to remember. This study specifically indicated that the issue of an individual recalling multiple passwords is a relevant and important factor in analyzing password strength. Further, the study found that it is difficult for an individual to memorize passwords with special characters and numbers, which are often specifically required in password policies.

Vu, Bhargav, and Proctor (2003) examined a specific policy in which thirty-two university students were asked to generate and remember passwords. Each participant was
granted multiple attempts to provide the correct password and those attempts were analyzed for recall. Participants’ memory recall was examined with focus given to the short term and long term across multiple accounts. In the short term memory recall it was found that passwords required an average of 2.8 attempts to login with five accounts and 1.4 attempts for three accounts. Also reviewed was the ability of an individual to memorize and recall a password after a specific amount of time had passed. Long term memory recall produced similar results with an average of 2.7 attempts for five accounts and 1.5 attempts for the three accounts recall. The passwords were then cracked using brute force algorithms in which over half of them were cracked within twelve hours. This shows that even passwords with low brute force strength were susceptible to coping mechanisms through low memorability.

Florencio and Herley (2007) from Microsoft Research analyzed the password use habits of 544,960 individuals over a three month period by utilizing an opt-in agreement through the Windows Live Toolbar that was first available for download on July 24, 2006. They found that the average user has 6.5 passwords, which is shared across 3.9 different websites; each user has an average of twenty-five accounts that require passwords, and on average, types eight passwords per day. They estimated that at least 1.5% of users forgot their Yahoo password every month. This study furthers the concern that users have multiple passwords to remember, utilize the same password across many sites, and in general, have problems remembering their passwords.

One study that seems to negate many of the concerns of users writing down passwords was completed by Shay et al. (2010). This review focused on 470 individuals from Carnegie Mellon University who were required to change their university passwords due to a system wide change in policy. While a much smaller percentage of the individuals (13%) wrote down his or
COPING MECHANISMS IN PASSWORD SELECTION

her password, a much larger percent (80%) reused a password and 50% reported modifying an old password to create the new one. Each of these are considered coping mechanisms that individuals can and do utilize in attempting to comply with password policies.

One additional coping mechanism that users often utilize is to choose a password that is similar to a security question provided by the organization. Many of the answers for these security questions are sometimes unknowingly available online from social media sites or similar resources. Often the answers to these security questions are guessable if knowledge of the individual is known. Whether the question is used to aid in remembering the password or used to verify an account for a password reset, attackers can exploit information found online to gain access to a user’s account.

**Entropy as a measurement of strength.** In order to create policies that will hopefully cause strong password creation by users, organizations use entropy to determine the strength of a password. A simple definition of entropy provided by Shay et al. (2010) is that it is the “measure of the difficulty of guessing a password.” In 2006, Burr, Dodson, and Polk at the National Institute of Standards and Technology (NIST) defined entropy as “A measure of the amount of uncertainty that an attacker faces to determine the value of a secret.” Thus, the greater the entropy, the more difficult it is for a hacker to predict the value of a variable, and therefore gain access to the protected information.

More specifically, the two main external types of threats to a password are password guessing and password cracking. Guessing comes in many different forms, including 1.) Brute force attacks where the attacker tries to guess the password by using all possible combinations of characters, 2.) Dictionary attacks where the attacker uses a list of works to try to guess the password, and 3.) The attacker searches for the user’s personal information, such as birthdays
and names, to attempt to guess the correct password. Password cracking attempts to create a string of hashes that has the same encrypted hash as the password. The password created by the new hash may or may not be the same as the users, but because the hash matches, the attacker is granted access.

Studies that have analyzed entropy have determined that numbers in a password add more entropy than lowercase letters (Komanduri et al. 2011). In addition, users tended to utilize more numbers in password creation than the policy imposed required. In this specific study, over 5,000 users created passwords under policies entitled Basic16 and Comprehensive8. Those passwords that were created were then evaluated by comparing the entropy. It was also found that users tested under the Comprehensive8 policy resulted in approximately 50% of the users storing their password. Those tested under the Basic16 policy resulted in approximately 33% of the participants storing their password.

Kelley et al. (2012) further expanded on the research by Komanduri et al. (2011), in utilizing different password cracking algorithms on a leaked password list and the data collected in the Komanduri study. The analysis reviewed both the guessability and entropy of passwords and allowed for an infinite number of guesses on each password. It was found that though NIST considers the password policies known as Basic16 and Comprehensive8 equivalent, Kelley et al. (2012) found that the Basic16 was the more secure against a large number of guesses. Basic16 requires the password to have at least sixteen characters, and Comprehensive8 requires a password with at least eight characters, an uppercase, a lower case, a symbol, and a digit. In addition, Comprehensive8 could not contain a dictionary word.

For a thorough overview of the accepted policies that provide a minimum level of security that is accepted for general use in the information security field, the researchers also
reviewed the work conducted by Horcher and Tejay (2009). This study examined the strength of a single policy against a dictionary attack and determined the distribution of time that it would take to crack passwords based on a pre-computed password list. Horcher and Tejay (2009) found that 93% of eight character passwords could be cracked within twelve hours using a dictionary attack.

**Cross-Cutting Studies.** In 2009, Scarfone and Souppaya at the NIST produced special publication 800-118, which describes in detail issues that affect password strength, common threats against passwords, and how to best mitigate those threats. While this document provides detailed and informative background information on password entropy and threats, as well as three types of password management technologies, there are no recommendations for policies that organizations should follow. Our work expands on this document by not only considering the most effective policies that provide the greatest strength, but also recognizes the coping mechanisms utilized by individuals.

Long term recall with multiple passwords was reviewed by Zhang et al. (2009) and compared to short term recall of one password. The study identified that recall of multiple passwords is a relevant and important factor in analyzing password strength. The authors found that it is difficult to integrate numbers and special characters into meaningful passwords that users will remember. Our work expands on this by proposing a data collection method which studies the historical changes in passwords, and how this affects a user’s ability to remember not only multiple passwords, but multiple password changes.

**Methods**

Participants for the study will be pulled from Purdue University’s Elementary Psychology courses. In these classes students are required to earn a specified number of credits
by participating in research studies. These studies may require a single one hour meeting or a recurring meeting that spans the semester. Most of these research studies require the students to physically be present at the testing area, though there are some that only require the student’s participation via the internet. Upon completion of these studies the student is awarded points for their participation that is a portion of their class grade.

For the purposes of this experiment we will not be requiring students to meet on campus. Everything will be completed online through a website that the students will visit and work through to fulfill their participation credits. This will allow students who are taking the course online through the extended learning program to participate, as well as increase the number of participants in the study. The students will be required to create an account through a website and return on a regular basis. Upon each visit the user will be prompted to login and complete a series of simple questions. The login and requirement to complete a simple question in order to receive participation credits will create a sense of priority in remembering to login and participate. This will help generate passwords that the participants are more prone to have created in a real world scenario.

Once the users have filled out the necessary information for their account, they will complete a pre-experiment questionnaire. These questions can be found in Appendix A. The questions will ask for participants to identify their gender, age, and their major or area of study. These pre-experiment questions can be used in the future for further analysis of password creation that will not be covered in this paper. Further, the participants will review and sign an informed consent that has been approved by an Institutional Review Board.

The participants will be assigned to one of the three password policies. As each user registers, she will be assigned to the next policy in line. For example, participant number one
will be assigned to Basic16, participant number two will be assigned to Comprehensive8, participant number three will be assigned to BlacklistHard, and participant number four will start the list over again, and be assigned to Basic16. A review of the research in the area of password strength indicates that control groups are not regularly used. Further, we intend to specifically review how each individual participant changes her password overtime, and the effects that those changes have on her reverting to coping mechanisms. A control group where the participants are not regularly required to change passwords will not provide the information that we are seeking.

Upon completion of the questionnaire, the participants will then be prompted to generate a password for the account using one of three policies selected for this experiment given in Table 1.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic16</td>
<td>Password must have at least 16 characters.</td>
</tr>
<tr>
<td>Comprehensive8</td>
<td>Password must have at least 8 characters that includes at least one: special character, number, uppercase letter, and lower case letter. The password cannot contain a dictionary word.</td>
</tr>
<tr>
<td>BlacklistHard</td>
<td>Password must have at least 8 characters and may not contain a dictionary word.</td>
</tr>
</tbody>
</table>

Basic16 requires the user to generate a password or passphrase that is at least sixteen characters long. The user is not required to include uppercase, lowercase, numbers, or special characters. Users are not restricted from including them in their password creation. This strategy will be helpful in analyzing whether the participant reuses a password from another policy or if he or she has developed a natural tendency to include these in her passwords.

Comprehensive8 requires a password of eight characters long and must include at least one: special character, number, uppercase letter, and lowercase letter. The user is then free to include any additional characters in order to meet the length requirement of eight characters.
The BlacklistHard policy requires a password with a length of eight characters and does not contain a dictionary word. The user is free to include or exclude numbers, special characters, uppercase letters, and lowercase letters in their password generation under the BlacklistHard policy. For the analysis, the password is not stripped of non-alphabetic characters in order to see the coping mechanisms a user may have implemented.

After the participant has set up her account and generated a password specific to her policy, she will be instructed on how the experiment is laid out. Regardless of the individual’s assigned policy, the research participant will be required to reset her password every two weeks. This is to gather historical data on the individual’s password generation and the coping mechanisms a participant may utilize over time that can only be observed from her password history. It is also to simulate the time parameter that much of the industry has as part of its password policy. The only requirement the three different password policies share is that when generating a new password, it cannot match any of the previously generated passwords exactly.

The participants will be required to log into the website twice a week, usually on days they have class, in order to answer a question. The questions can be as simple as “Who is the current president of the United States of America?” or if the instructor wishes, the questions can be pulled from the course itself. This will require the participants to recall their password and log back into the website on a regular basis. Upon completion of the question task, the participant will be awarded part of the required research participant credits. The students will be able to track their points awarded from this website. This too will put an emphasis on the importance of the account that has been set up along with the individual’s participation in the study since her grade depends on it.
Participants will be sent reminder emails to complete their tasks every week. Failure to complete any login or task will result in a forfeiture of the points for that task.

If the user forgets her password, she will be allowed three attempts to login. After each attempt she will be prompted with a window that states “Login Failed! You have used one of three attempts allowed.” After the third failed attempt the user will be prompted with the option to recover her password. The participant will need to type her chosen email address into the prompt box, verify the email address is correct by typing it again into a second box, and then hitting “ok” to confirm she wants to have the password sent to her account. The password will be sent to the email provided and the user is then free to try and login again. Each participant will be given three more attempts to login after having her password sent to their email. Once successfully logged on, the user will then be prompted to create a new password before she can continue on to her quiz to earn research credit. These password resets will be recorded so that they can be analyzed as an anticipated coping mechanism. As much of the industry has lock out periods from failed logins, these recorded password resets can be used for cost analysis of money and time wasted. Further, an analysis could also be conducted of whether there is a correlation between the number of password resets and coping mechanisms.

At the end of the research study, the participants will be required to participate in a survey in order to earn their credit for the Psychology 120 course. Example questions for this survey are given in Appendix A. These questions ask the participants to detail any coping mechanisms they relied upon throughout the semester.

For each profile created on the website, the participants’ age, sex, and major or area of study will be saved. Each password used for this profile will be saved in the order they were generated to establish a chronological order to her password generation. Any failed login
attempts will be noted and linked to the profile. Any passwords generated from a reset request for the user profile will be saved. The completion of the question once logged in will be saved to show the user had successfully logged in and earned her research credit. This time and date stamping can be used for further analysis that is outside the scope of this project. Data for each participant will be saved and exported as an Excel sheet. The participant's name will not be linked to this data to insure anonymity.

**Results**

The Data Collection Method will be put into place during the next course, so at this time, we do not have any data to review or results to report.

**Discussion**

Three policies were selected to be examined in the study to be performed in Fall 2014. These policies were selected based on several criteria, including real world relevance, strength, scope, and participant password experience.

The first priority in the selection of the policies is the potential for providing meaningful data on the coping mechanisms. It was also important for the password policy to be of sufficient strength, and potentially in use at organizations today. Thirdly, the password policies were selected based on the scope of the passwords that the user can produce ranging from one word toward random characters.

The Comprehensive8, Basic16, and BlacklistHard policies all have a relatively similar strength based on the NIST model for entropy, as is noted in Table 2, but each represents a certain extreme of a policy. In addition, each policy provides information of how a user will choose a password to satisfy a particular policy and how that password will change over time. While each policy gives instructions for what is required for a password (symbols, capital
letters, etc) the participant is allowed to use any character on the keyboard. This will allow researchers to examine the user history to see if the special characters or numbers can be used as coping mechanisms.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Random Assignment Keyspace</th>
<th>Random Assignment Entropy</th>
<th>NIST Entropy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comprehensive8</td>
<td>6.09569E+15</td>
<td>52.43671081</td>
<td>30</td>
</tr>
<tr>
<td>Basic16</td>
<td>3.71574E+31</td>
<td>104.8734216</td>
<td>30</td>
</tr>
<tr>
<td>BlacklistHard</td>
<td>6.09569E+15</td>
<td>52.43671081</td>
<td>24</td>
</tr>
</tbody>
</table>

When calculating the strength of a policy using the NIST method or for the keyspace of possible passwords there are certain limitations of what is and is not covered within the policy. The keyspace, which is the number of total possible passwords that could be created based on each specific policy, reflects the lowest possible character length. It is shown that the average character length in policies similar to the average length of the user password is at least two characters longer than the minimum length requirement (Vu, Bhargav, and Proctor 2003). This indicates that the keyspace of a password is not being correctly considered during entropy calculations. Entropy calculated through NIST metrics is determined by calculating the length of the password with the first character representing four bits of entropy, the second through eighth characters representing two bits of entropy each, and the ninth through twentieth characters representing one and a half bits of entropy each. Additionally, if a password contains upper case letters and special characters it is given an extra six bits of entropy. The same is given for a password that is not a dictionary word.

Passwords created by users in this data collection method will be analyzed for entropy and coping mechanisms to see how far outside the policy passwords truly fall. Then, coping
mechanisms will be identified and linked to each user password as the password evolves over time in response to the biweekly changes. Data stored will be the self reported coping mechanisms given in the user surveys as well as the coping mechanisms identified by the research examiner. This data will show when the user started using coping mechanisms, if and when the user admits to using coping mechanisms, and how extensive the use of the coping mechanism is.

As the passwords collected will not be encrypted, there is no anticipation at this point to utilize guessing or cracking attacks. It will be important for the researchers to have the actual passwords created, instead of hashes, to be able to determine whether incrementing or doubling is occurring.

The greatest information gained in this research will be the data regarding the participant’s use of coping mechanisms. Many different studies have hinted at a concern of password policies becoming too stringent and frustrating for users. However, there has not been data collected on a large scale over a multi-week time frame, with required password changes built in, with a large number of participants. This novel information will provide data that can be analyzed with regard to when an individual starts using coping mechanisms, which coping mechanisms are the most widely used, which policy leads to participants using the most coping mechanisms, and whether any of the policies’ strength was undermined by the coping mechanism used.

Conclusions

It is clear that restrictive password policies can lead to users reverting to coping mechanisms, which can decrease the effectiveness of the security. Further, many studies have reviewed password strength and hacking tools in an attempt to determine the strongest password
policy. However, it is not known how multiple password changes over time will affect utilization of coping mechanisms, or how these coping mechanisms weaken the policy and increase user frustration. Our data collection method and proposed analysis will provide a metric to collect the data on these subjects, to hopefully provide a recommendation for an effective, but not overly burdensome, password policy.

**Current and Future Recommendations**

Current studies indicate that Comprehensive8 and Basic16 have the greatest entropy. In addition, BlacklistHard tested well in terms of guessability. When comparing the composition of these policies, Basic16 provides the users with the greatest opportunity for memorability, as an individual does not need to keep track of special characters, capital letters, or numbers. Basic16 also allows a person to use a phrase as opposed to a word, which also can increase memorability.

Future recommendations are to utilize the data collected in this study for analysis of demographic password creation as well as cost analysis for an organization when users forget their passwords. This data may also be useful when making administrative and policy decisions to adopt other security measures such as Smart Cards, Biometric options, Radio-Frequency Identification, or hardware tokens, to be used in conjunction with passwords. With these other security measures in place, an organization may be able to adopt a less stringent password policy, which will be less frustrating for the user, but increase the security of the information.
References


Shay, R., Komanduri, S., Kelley, P., Leon, P., Mazurek, M., Bauer, L., Cristin, N.,

on Usable Privacy and Security (SOUPS), Redmond, WA.

multiple accounts: Impact on generation and recall of passwords. Proceedings of
the 47th Annual Meeting of the Human Factors and Ergonomics Society, 1331-1335.
Santa Monica, CA: HFES.

Password Recall: an empirical study. European Journal of Information Systems, 18(2),
165.
Appendix A

Entrance Survey Questions:
1. What is your gender?
2. What is your age?
3. What is your major/course of study?
4. Where were you born?

Task questions will be to answer a single question each day, comprised of the following:
(Note: these may be replaced by coursework questions if the professor chooses.)
- What day is today?
- What is your favorite color?
- Have you ever had a pet?
- What is your favorite movie?
- What is your favorite book?
- Do you like pizza?
- What color is your residence?
- What is your favorite college football team?
- What is your favorite college basketball team?
- What is your favorite professional baseball team?
- Do you like sports?
- Do you like to read?
- Have you ever traveled outside of Indiana?
- Are you from Indiana?
- What is your favorite food?
- What color is your shirt?
- Is it raining today?
- Is it sunny today?
- What is the name of the President of the United States?

Exit Survey Questions:
1. Have you ever used the same password to access multiple accounts?
2. Have you ever slightly modified a password to comply with a change in password policy within the same account?
3. Have you slightly modified a password when facing a routine change of password requirement instead of creating or utilizing an entirely different password?
4. Have you ever utilized any personal information such as a pets name, the street where you grew up, a middle name, date of birth, etc., to assist you in creating a password?
5. Have you ever written down a password for any reason?
6. Did you utilize the same or similar password in this exercise that you used on another account?
7. Did you slightly modify your password when facing the routine change of password requirements instead of creating or utilizing an entirely different password?
8. Did you write down a password during this exercise?
9. If you wrote down a password at any point, please indicate the reason, time frame, and the number of times the password was written down.
10. If you wrote down a password, did you store it electronically or on paper?
11. Did you utilize any personal information, such as a pet’s name, the street where you grew up, a middle name, date of birth, etc., to create your password in this exercise?
12. Why did you choose your password? (categorize passwords, I.E. important name, significant numbers…)