Encountering Stronger Password Requirements: User Attitudes and Behaviors

Richard Shay
rshay@cmu.edu

Saranga Komanduri
sarangak@cmu.edu

Patrick Gage Kelley
pgage@cmu.edu

Pedro Giovanni Leon
pedrogln@cmu.edu

Michelle L. Mazurek
mmazurek@andrew.cmu.edu

Lujo Bauer
lbauer@cmu.edu

Nicolas Christin
nicolasc@cmu.edu

Lorrie Faith Cranor
lorrie@cmu.edu

Carnegie Mellon University
Pittsburgh, PA

ABSTRACT

Text-based passwords are still the most commonly used authentication mechanism in information systems. We took advantage of a unique opportunity presented by a significant change in the Carnegie Mellon University (CMU) computing services password policy that required users to change their passwords. Through our survey of 470 CMU computer users, we collected data about behaviors and practices related to the use and creation of passwords. We also captured users' opinions about the new, stronger policy requirements. Our analysis shows that, although most of the users were annoyed by the need to create a complex password, they believe that they are now more secure. Furthermore, we perform an entropy analysis and discuss how our findings relate to NIST[†] recommendations for creating a password policy. We also examine how users answer specific questions related to their passwords. Our results can be helpful in designing better password policies that consider not only technical aspects of specific policy rules, but also users' behavior in response to those rules.

Categories and Subject Descriptors

D.4.6 [**Security and Protection**]: Authentication; H.1.2 [**User/Machine Systems**]: Human factors

General Terms

Security, Human Factors

[†]National Institute of Standards and Technology

Keywords

Security, Usability, Passwords, Policy, Survey

1. INTRODUCTION

One of the fundamental problems in computer security is how to authenticate a user to a computer system conveniently and securely. Authentication is typically the first step toward confirming that a user is authorized to perform a requested action, be it retrieving email, withdrawing money from an ATM, or issuing commands to a power-distribution grid.

In recent years, a number of devices and techniques have been proposed—including smart cards, RFID cards, USB tokens, and graphical passwords—to make authentication more usable, convenient, and secure. While each of these technologies has its advantages and may be well suited for use in a specific environment or for a specific application, text-based passwords remain the most commonly used authentication mechanism. This is in part because text-based passwords require no special hardware and are easy for end users to input and for system developers to implement.

Compared to more recent authentication technologies, such as those that rely on public key cryptography, text-based passwords are often seen as being less secure—easier to predict or guess for an adversary—thereby making it possible for the adversary to impersonate a legitimate user and misuse his or her authority. In large part, this weakness of text-based passwords is due to their brevity.

The issue of text-based passwords being drawn from a relatively small space is compounded by the propensity of users to select particularly weak passwords, such as those containing or based on dictionary words. This means that the space of passwords actually used is much smaller than the space of theoretically available passwords, dramatically increasing the likelihood of an attacker being able to discover a given password, through a brute-force attack or even guessing.

To combat both the inherent and user-induced weaknesses of text-based passwords, administrators and organizations typically institute a series of rules—a password policy—to which users must adhere when choosing a password. A pass-

word policy may specify, for example, that a password must have a minimum number of characters, that it must include uppercase letters or numbers, and that it may not include dictionary words. The purpose of such password policies is to ensure that the space of possible passwords is large and to prevent users from selecting passwords that may be easy for an attacker to discover, whether by guessing or through a brute-force attack.

There is consensus in the literature that a properly written password policy can provide an organization with increased security [10, 20, 21, 22, 23]. There is, however, less accord in describing just what such a well-written policy would be, or even how to determine whether a given policy is effective. Prior work has examined user habits with passwords [7], simulated users [20, 21], performed laboratory experiments [14, 23], studied lists of passwords [1], and surveyed users with a static password policy [11, 16, 17, 24]. Despite this work, the effects of password policies are still unclear, for two main reasons, detailed below.

First, although it is easy to calculate the theoretical password space that corresponds to a particular password policy, it is difficult to determine the practical password space. Users may, for example, react to a policy rule requiring them to include numbers in passwords by overwhelmingly picking the same number, or by always placing the number in the same location in their passwords. There is little published empirical research that studies the strategies used by actual users under various password policies.

Second, some password policies, while resulting in stronger passwords, may make those passwords difficult to remember or type. This may cause users to engage in a various behaviors that might compromise the security of passwords, such as writing them down, reusing passwords across different accounts, or sharing passwords with others. Further undesirable side effects of particular password policies may include frequently forgotten passwords, which may increase help-desk workload and thus IT-support costs [15]; discontent among users forced to adhere to an inconvenient password policy; and generally diminished productivity [6, 7]. In fact, the harm caused by users following an onerously restrictive password policy may be greater than the harm prevented by that policy [6].

In this paper, we seek to advance understanding of the factors that make creating and following password policies difficult. We present the results of a survey of 470 Carnegie Mellon University (CMU) students, faculty, and staff, conducted soon after the university's password policy underwent an abrupt change from being very unconstrained, to being very constrained. Because of this opportune timing, we were able to gather data to compare user habits under both policies. We also gathered users' impressions shortly after they experienced the policy shift and collected information on password-selection strategies under the new policy.

Among our findings is that, unsurprisingly, users were annoyed by the shift to a stricter password policy. However, we also found that users did not find it difficult to adhere to this policy and believed that the change in policy resulted in greater security. Users were neutral toward whether the change was worth the effort, and whether CMU should return to its prior password policy. Relatively few users wrote down their passwords, but a significant number reused their passwords across accounts or shared them with others. In analyzing these and other findings we also discovered statistically significant differences between the behavior of different demographic groups.

Our investigation included collecting statistics about some very specific password-selection behaviors, such as which digits users opted to use and the locations of these digits in passwords. Roughly extrapolating from these results, we estimate the practical entropy of passwords that adhere to the new policy.

This paper is organized as follows. In Section 2, we discuss the change in CMU's password policy in more detail and review related work. We describe the methodology of our study in Section 3. In Section 4, we present our results on user behavior: we report on demographics, user sentiment, how users fared in creating and memorizing passwords, and the sharing and reuse of passwords. In Section 5, we present our findings about users' password-construction strategies, the entropy of passwords created under the new password policy, and how this entropy compares with that predicted by NIST. In Section 6, we highlight our most significant findings.

2. BACKGROUND AND RELATED WORK

In this section, we provide more detail about the Carnegie Mellon password policy change and discuss related work.

2.1 CMU Password Policy Change

CMU students, faculty, and staff have accounts on the Andrew computer system. These password-protected accounts provide access to important online services, including email, course registration, and access to licensed software. Until the end of the Fall 2009 semester, the only password requirement enforced for most Andrew users was that their password include at least one character.

In December 2009, all Andrew users received an email announcing a new, stricter password policy. By January 27, 2010, all Andrew passwords would be required to contain at least eight characters, and include at least one uppercase letter, one lowercase letter, one digit, and one symbol. Furthermore, new passwords would be subject to a dictionary check: if the string obtained after removing all non-alphabetic characters matched a dictionary word, the password would be rejected. Passwords containing four or more occurrences of the same character would also be rejected.[1]

When the new password policy went into effect on January 27, users without compliant passwords became unable to access their Andrew accounts. By that evening, 88.2% of the 14,587 student accounts were compliant, as well as 82.8% of the 4,511 staff accounts and 78.6% of the 2,005 faculty accounts. Some users may have failed to change their passwords because they no longer used their Andrew accounts.

This change in password policy was motivated by the university's joining the InCommon Federation, "a formal federation of organizations focused on creating a common framework for collaborative trust in support of research and education."[2] The federation has entropy requirements for passwords for achieving specific identity-assurance levels: for example, achieving bronze or silver identity-assurance status

---

[1] www.cmu.edu/computing/news/status/andrew/
[2] www.incommonfederation.org

requires the probability of successfully guessing a password be no more than 1 in 1,024 or 1 in 16,384.[3]

To create a silver password policy, CMU systems administrators used a government-issued password-entropy calculation spreadsheet.[4] This spreadsheet, which associates various password policy configurations with estimated per-password entropy, is based on National Institute of Standards and Technology (NIST) guidelines for estimating how many attempts are required to guess a password under a given policy [2].

2.2 Related Work

Several studies have examined how password policies affect users. In a study using password diaries, Inglesant et al. identified tradeoffs between password strength and productivity at work. They found that although users were aware of the security concerns that influence password requirements, users rarely changed their passwords, and password policies did not account for sensitivity variations in the resources they protect [7]. This work, like ours, used feedback from real users to examine the effects of password policy. Unlike our survey, however, this study focused on gathering detailed information from a small set of users.

Leyden reported on an informal survey in which 90% of 152 computer system users divulged their passwords in exchange for a pen. The survey also found that users tended to use simple passwords, with "password" itself used 12% of the time [11]. A SafeNet survey asking thousands of users about their security habits and their organizations' security policies found that about half of the respondents wrote down their passwords and about 80% had three or more passwords [16].

Surveying 123 computer science undergraduates on password sentiment, Hart et al. found most were not concerned about password security. Around 20% of students shared their passwords and about 30% used the same password four or more times [5]. Our survey, unlike that of Hart et al., included faculty and staff as well as students, and was administered to a larger set of users.

In a 1999 survey of computer users at a Department of Defense installation in California, Zviran and Haga collected user demographics, computer usage information, and password characteristics from 860 people, and then explored associations within the data. They found that the most common password length was six characters, 80% of users had entirely alphabetic passwords, 80% never changed their passwords, and 35% never wrote their passwords down. They found no association between password composition and the sensitivity and importance of the data being protected or between the method of selecting a password and the importance of the data [24]. In the Zviran and Haga study, unlike ours, users did not seem to be required to observe a strict password policy.

Shay et al. used computer simulation to analyze the results of various password policies on overall organizational health. The results indicated that although a password policy that allows weak passwords can lead to system compromise, an overly strong policy can lead to users writing down passwords and thereby increase system vulnerability [20,21].

Other prior work has examined password policies using laboratory studies. Proctor et al. and Vu et al. found that passwords made under stronger restrictions can be harder to crack using automated tools but also harder to create and remember [14]. Vu et al. also found that that the likelihood of remembering a specific password diminished as more passwords were remembered [23]. Bishop et al. used automated tools to investigate the difficulty of cracking real password files provided by systems administrators [1].

Kuo et al. found that automated cracking tools were less successful against mnemonic passwords than against control passwords. Also, the authors demonstrated the feasibility of building mnemonic password dictionaries based on popular phrases [10]. Kuo et al. examined passwords created specifically for the study, as compared to our survey of passwords in regular use by users.

Using an opt-in component of the Windows Live Toolbar, Florencio et al. captured password information for more than half a million people. On average, each person used seven passwords across 25 different websites. The authors found that the strongest passwords were used on just a few websites, while weaker passwords were reused more often [3]. Florencio et al. examined passwords across a wide variety of account types and unspecified password-strength requirements; our study, by contrast, focuses on a specific password policy. Our study also considers user sentiment toward password policy in addition to password strength and reuse.

Our work also differs from each of the mentioned studies in that we considered users of one specific system just as a less constrained password policy was replaced by a more constrained one. As a result, we gathered data about a single set of users in one system under two very different password policies.

3. METHODOLOGY

In February 2010, we conducted a paper-based survey of 470 CMU students, faculty, and staff who had changed their Andrew password to comply with the new requirements. We designed our survey to collect data on password handling, password composition, password storage and reuse, and user sentiment about the new password requirements. In this section, we discuss our survey design, our survey questions, and our survey administration and analysis process.

3.1 Survey Design

We set out to design a survey that would elicit truthful information about passwords from a cross-section of university students, faculty, and staff. While collecting and managing the data would have been easier online, we were concerned that more security-savvy users would be reluctant to provide truthful information if they thought we could link their responses to their usernames. The CMU Information Security Office (ISO) also expressed concern that an online survey asking users to divulge information about their passwords would conflict with advice in their cyber-security awareness campaigns and confuse users. Therefore, we opted to conduct the survey on paper, asking passersby on the CMU campus to complete survey forms.

We designed the survey form to fit on both sides of a single sheet of paper and expected that typical participants would take about four minutes to complete it. In order to keep the survey short, we limited the number of questions we asked in each category and did not include any open-ended questions.

---

[3] www.incommonfederation.org/docs/assurance/InC_Bronze-Silver_IAP_1.0.1.pdf

[4] www.idmanagement.gov/eauthentication/drilldown_ea.cfm?action=ea_credsuite

While pilot testing the survey, we received feedback that our password composition questions made respondents uncomfortable. Pilot testers expressed concern that we were gathering so much specific data about their passwords that we might be able to determine them. We feared that these concerns would prevent users from taking our survey or cause them to answer untruthfully. To reduce the amount of information we might collect about any given user's password, we created two variants of the survey form, A and B, and divided the password-composition questions between them. In addition, for questions that users might have been uncomfortable answering, we included an "I prefer not to answer" option.

3.2 Survey Questions

We give an overview of our survey questions here. We provide the front of the survey form and the A and B variants of the back in Appendix A.

Demographics We asked four demographic questions: role at CMU, gender, age, and whether the respondent was majoring or had a degree or job in the information technology (IT) field.

Password Handling Next, we asked eight questions about when and how respondents created their password and how they have handled it since. Respondents were first asked when they changed their passwords to comply with the new policy. The response options included "I have not changed my password to comply with the new policy yet." Surveys with this response indicated were dropped from the results, since the target population was users who had complied with the new policy. Respondents were asked, "If you tried to login to your Andrew account right now, how many attempts do you think it would take?" to gauge their confidence in recalling their password. Respondents were also asked whether and with how many people they shared their old and new passwords, and whether they had forgotten their new password and, if so, how they recovered it. We asked two questions about strategies used in creating their new password. Finally, all respondents were asked how many tries it took to create an acceptable password.

Password Composition All respondents were asked the length of their passwords and which symbols they used. Survey A asked how many uppercase and lowercase letters were used, and in which positions numbers and symbols occurred. Survey B asked how many symbols and numbers were used and in which positions uppercase letters occurred. Each of these questions included the response option of "I prefer not to answer."

Password Storage and Reuse Respondents were asked whether they have written down their current password, either on paper or electronically. If so, they were asked to indicate how it is protected, selecting from eight response choices including, "I do not protect it" and "Other" followed by a blank line. The question was then repeated for their old password. Respondents were then asked if they have a set of passwords they reuse and whether they have a password for different accounts reused with slight modification.

User Sentiment Finally, respondents are presented with six Likert questions concerning their sentiment regarding the policy change. Five of the questions were constant between surveys. Survey A asks users "Creating a password that meets the new requirements was difficult" while survey B replaces the word "difficult" with "easy." Other questions included "With the new password requirements, my Andrew account is more secure", "Creating a password that meets the new requirements was annoying", "Creating a password that meets the new requirements was fun", "Any added protection provided by the new password is worth the added effort of creating/remembering/using it", and "I would like Andrew to go back to the old password policy". Response options for all six questions were "Strongly Agree", "Agree", "Neutral", "Disagree", and "Strongly Disagree".

3.3 Survey Administration and Analysis

We distributed surveys within a two-week period in February 2010, soon after the January 27 password-change deadline. Researchers went to areas on the CMU campus where students, faculty, or staff were likely to congregate, including the student center, dining areas, library, classroom buildings, and department offices. Potential respondents were approached by researchers and asked if they would like to take a survey. If asked, researchers told respondents that the survey was about the recent password policy change. Respondents were offered a selection of candy bars and snacks for their participation. Having the same group of researchers handing out surveys, all within a short period of time, helped prevent participants from taking the survey more than once.

We entered the responses to each survey form into an online survey management system. Before conducting a detailed analysis of the results, we disqualified surveys in which the respondent indicated that he or she had not yet changed his or her password. We also disqualified surveys in which the respondent answered the password composition questions in a way that was inconsistent with the new requirements (for example, some respondents said their new password was fewer than eight characters or did not contain a symbol or a number). Some participants opted against answering all questions on the survey, either by leaving a response choice blank or by selecting the "I prefer not to answer" response choice when available. We did not disqualify any surveys for blank responses.

4. USERS AND THEIR BEHAVIOR

We collected 492 surveys and disqualified 22 of them based on the criteria described in Section 3.3. This section presents results about user behavior based on our analysis of the remaining 470 surveys. We first detail the demographics of our participants, followed by our findings related to user sentiment. We next describe how users transitioned to the new password policy, coping strategies they employed, and their tendency to share their passwords. Finally, we examine the rate of user refusal to answer our password composition questions.

4.1 User Demographics

We categorized participants according to gender, age, role on campus, and IT experience. Since a large number of our participants were undergraduate students, we focused our analysis on two age groups: those under 22 (mostly undergraduates), and those 22 and older (graduate students, faculty, and staff). As illustrated in Figure 1, the mean age for students (21.0) is significantly different from the faculty (38.2), staff (50.4), and "other" (29.3) groups ($p < 0.0001$, Kruskal-Wallis test). IT experience was evaluated by asking, "Are you majoring in or do you have a degree or job in computer science, computer engineering, information tech-

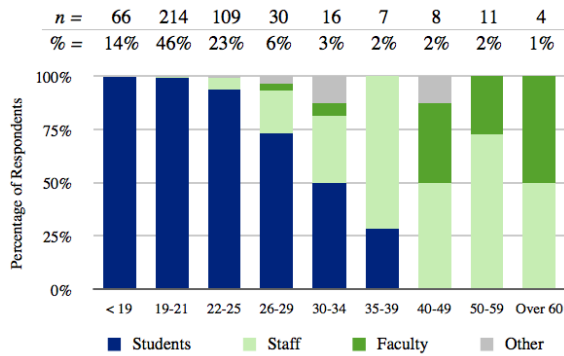|	Number	Percent
Gender		
Male	228	48.5%
Female	241	51.3%
No Answer	1	0.2%
Age		
<22	280	59.6%
≥22	185	39.4%
No Answer	5	1.1%
Role		
Faculty	10	2.1%
Staff	41	8.7%
Student	413	87.9%
Other	6	1.3%
IT Major/Job		
Yes	162	34.5%
No	301	64.0%
No Answer	7	1.5%

Table 1: Participant demographics

Figure 1: A comparison of university role and age.

nology, or a related field?". Table 1 and Figure 1 summarize the basic demographics of our participants.

These four demographic groups are not independent. For example, while 73% percent of IT participants are male, only 35% of non-IT participants are; this difference is significant ($p < 0.0001$, Fisher's exact test, or FET). Additionally, when looking at the relationship between students and other participants, both the male/female dichotomy and the percentage of IT experienced participants are significant ($p < 0.0001$, FET). These relationships between our demographic groups are shown visually in Figure 2.

Our survey sample is not entirely representative of the CMU population or the population of Andrew account holders, which is 70.6% student, 8.6% faculty, 20.5% staff, and 0.2% other. In our sample, faculty and staff are somewhat underrepresented. In addition, while the CMU student population is 64% male,[5] the students in our sample were only 52% male. Our ratio of males to females differs significantly from the CMU population (χ^2 test, $p-value < 0.0001$).

4.2 User Sentiment

Survey respondents reported their opinions on the password policy change by responding to six 5-point Likert ques-
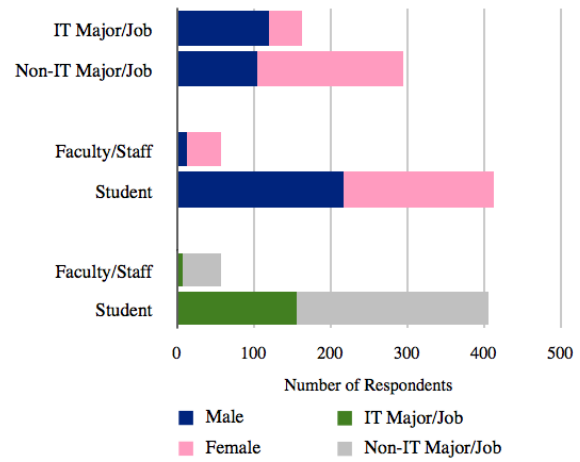
Figure 2: Significant relationships among demographic constituents. All relevant $p-values < 0.0001$.

	Mode	Mean	Std. Dev.
Secure	4 (agree)	3.6	0.92
Easy†	4 (agree)	3.2	1.09
Annoying	4 (agree)	3.7	1.05
Fun	2 (disagree)	2.2	0.97
Worth the effort	3 (neutral)	3.4	0.96
Back to old system	3 (neutral)	2.8	0.91

Table 2: Participant responses on a Likert scale (1 being "strongly disagree," 5 being "strongly agree"). †For "Easy," approximately half of the participants were assigned each phrasing of the question; for this table, results for the "difficult" phrasing were reversed and combined with "easy."

tions. The responses are summarized in Table 2. Overall, respondents did not have strong feelings about the policy change.

Our first question attempted to gauge perceptions of the overall value of the password change, with respondents agreeing somewhat that their accounts are more secure as a result of this change. Respondents also indicated that they found the process of creating a new password fairly easy. On the other hand, respondents also found the password change somewhat annoying and disagreed that creating a new password was fun.

The overall acceptance that the new requirements improve security combined with the sentiment that changing passwords was annoying helps to explain the overall neutral responses about whether it was worth the effort to switch and whether the Andrew system should switch back to the old policy.

Opinions on whether the password change was easy or difficult were consistent across the two survey versions; participants agreed that the change was easy and disagreed with it being difficult. A Wilcoxon test with continuity correction and $\mu = 3$ indicates that the questions appear to be symmetric ($p = 0.25$).

We found only one significant difference in user sentiment results among demographic subgroups: IT participants were significantly more opposed to the idea of returning to the old policy (mean 2.6) compared to non-IT participants (mean

	1	2	3	4	Attempts 5	≥6
To create	59.6%	21.3%	11.1%	2.8%	3.7%	1.5%
To login	79.4%	17.1%	3.3%	0%	0.2%	0%

Table 3: Number of attempts respondents reported needing to create a new password and number of attempts they expect it would take to log in using that new password.

	Forgot	Had not forgotten		
Total Participants	87	375		
			chi-squared	p-value
Tries to create	2.3	1.7	13.97	0.0019
Tries to log in	1.5	1.2	24.11	<0.0001
			W	p-value
Annoying	4.2	3.6	$1.1 \cdot 10^4$	<0.0001
Fun	1.9	2.2	$1.9 \cdot 10^4$	0.0116

Table 4: Significant participant comparisons between users who have forgotten their passwords and those who have not. Kruskal-Wallis tests were used to compare "Tries" and Wilcoxon tests were used for Likert values. Holm-corrected $p - values$ are shown.

2.9). This difference, calculated using a Wilcoxon test with continuity correction, yields a Holm-Bonferroni-adjusted $p-value$ of 0.0048.

4.3 Transitioning to the New Policy

We examined how users transitioned to the new password policy, focusing on how they fared in creating and memorizing their new passwords.

Twenty percent of participants changed their password the same day they received the first request email; another 32% did so before receiving a second email. Forty-six percent changed after receiving multiple emails.

Participants reported that it took on average 1.77 tries to create a password the system accepted. Participants also expect it would take 1.25 tries to log in with their new passwords. These responses are detailed in Table 3.

Our results depict a portion of users appearing to struggle with the policy change; this is consistent with previous research that has shown more complex passwords to be more difficult to recall [9]. Eighty-seven participants, or 19%, reported forgetting their new password. These users show a number of significant differences from users overall, as shown in Table 4. They reported needing significantly more attempts to create and log in with a password under the new policy. They also found creating a new password more annoying and less fun.

Among users who had forgotten their current password, 60% recovered it by remembering it later, 21% retrieved it from where it was written, and 11% went to the help desk to have it reset. As might be expected, those who had forgotten their password were also four times more likely to have written their current password down.

Using a logistic regression model, we determined that the likelihood of forgetting the current password was related to several demographic factors. Faculty and staff were three

	Current Password	Old Password
I do not protect it	31%	18%
I hid it	16%	20%
I stored it on a computer or device protected with another password	13%	24%
I stored it in an encrypted file	11%	11%
I locked up the paper	9%	4%
I wrote down a reminder instead of the actual password	7%	16%

Table 5: How users protected their written-down passwords.

times more likely to have forgotten their passwords than students ($\beta = 1.134$, $p = 0.025$). Women were almost twice as likely to forget as men ($\beta = 0.627$, $p = 0.029$), and those who changed their password early were less likely to forget it ($\beta = 0.566$, $df = 2$, $p = 0.002$). Forgetting was not significantly related to IT experience or age.

4.4 Coping Strategies

Several survey questions concerned how users are coping with the policy change. These questions asked about password reuse between accounts and writing passwords down.

More than 80% of participants (381) reported reusing a set of passwords in different places. A total of 281 users said they use one password with slight modification for different accounts. Most of the users who reuse a set of passwords also use one password with slight modification on different accounts (254 of the 381). Women were more likely than men to reuse a password with slight modification: 69% of women compared to 55% of men ($p = 0.021$, FET).[6]

Only 63 participants (13%) reported writing down their current password, 40 on paper and 23 electronically. Fifty-six (12%) had written down the old password. Only 27 people wrote down both passwords; almost half of those are faculty or staff. Table 5 details how users who wrote down their passwords protected them.

Table 5 shows that although similar numbers of users wrote down old and new passwords, users took more precautions to secure their old passwords. This may result from newer passwords not being as well memorized due to their novelty or their complexity; users may keep them in a less secure location because they consult them more frequently.

A survey conducted in 2004 found that approximately half of surveyed employees wrote down their passwords [16]. Another survey conducted by Zviran et al. reported 65% of employees writing down their passwords [24]. These figures are larger than the 13% of users who did so in our survey. While many previous papers have discussed the phenomenon of users writing down their passwords [1,4,21,23,24], we observed users writing down their password to be less common than users reusing passwords.

4.5 Password Sharing

One hundred and twenty-seven participants (28%) said they had given their old or current password to at least one

---

[6]This result is also supported by a logistic regression analysis including gender, age, role on campus, and IT experience. Of these, only the coefficient of gender was significant ($p \approx 0.001$) with all other coefficients not significant (p > 0.1).
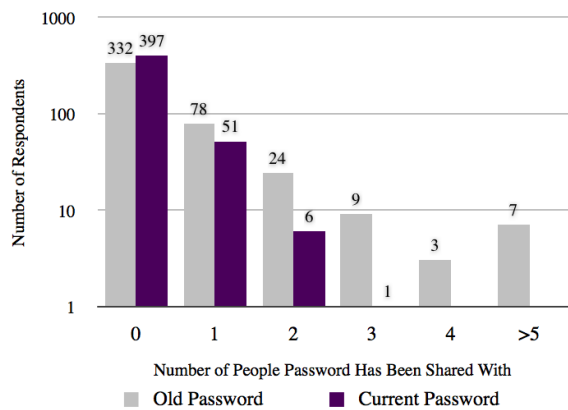
Figure 3: A comparison of sharing for old and new passwords.

Question Summary	Percent Answering
$Q13$. Password Length?	73%
$Q14$. What symbols in password?	46%
$Q15A$. How many lowercase letters?	65%
$Q16A$. How many uppercase letters?	68%
$Q17A$. In which positions are numbers?	65%
$Q18A$. In which positions are symbols?	66%
$Q15B$. How many symbols?	62%
$Q16B$. How many numbers?	66%
$Q17B$. In which positions are uppercase letters?	66%
$Q18B$. Contains number related to year created?	88%

Table 6: Proportion of participants who answered each question (out of the number of participants who took each survey version). Question summaries are given; their full text is found in Appendix A.

other person. Figure 3 illustrates how many people these passwords were shared with.

Fifty-two participants shared both their old and current password, sixty-seven participants shared only their old password, and six shared only their current password. This discrepancy may indicate that, since the current passwords are relatively new, occasions to share them have been less frequent. Overall, IT participants were less likely to share passwords with other people ($p < 0.0001$, Holm-corrected FET). Thirty-three percent of participants younger than 22 (our "undergraduate" group) shared their passwords, compared with 20% for the rest of the participants. This indicates that undergraduates are more likely to share ($p = .027$, Holm-corrected FET).

4.6   Refusal to Answer

One potential sampling bias for a voluntary survey such as this is that there may be a tendency for less security-minded users to participate. Furthermore, among survey respondents, security-minded users may be more likely to refuse to answer security-sensitive questions. A number of questions in the survey asked about the structure of the password (e.g., the position of the required symbols in the password, or the nature of these symbols). All of these questions had an "I prefer not to answer" choice, leaving the door open for respondents to refuse to answer. We also assume that a respondent who left a question blank was refusing to answer.[7] We next turn to an analysis of the patterns we observed in the refusals to answer.

In this analysis, participants are separated into *full disclosure* and *minimal disclosure* groups. This corresponds to answering all or none, respectively, of the subset of questions dealing with password structure.[8] One hundred and

nine participants answered all these questions (full disclosure group), while 69 did not answer any of them (minimal disclosure group). The rest of the participants (292) answered some, but not all of the questions.

We found that participants in the full disclosure group were more likely to reuse their passwords: 92% of them acknowledged that they do, significantly more than the 81% of people reusing passwords outside of the full disclosure group ($p = 0.011$, FET). Conversely, in the minimal disclosure group, only 66% of participants indicated they reused their passwords, significantly less ($p = 0.0002$, FET) than the 86% of participants outside the minimal disclosure group. In short, the more defensive a user is about sharing innocuous, but specific, password information in a survey, the less likely he or she is to engage in the practice of reusing passwords.

A secondary finding was that IT people were less likely to disclose the structure of their passwords. The full disclosure group contained only 23% IT people, while the rest of the sample contained 39% IT people ($p = 0.004$, Holm-corrected FET). Likewise, IT people make up 54% of the minimal disclosure group, while the rest of the sample contains the significantly lower proportion of 32% ($p = 0.031$, Holm-corrected FET).

The proportion of participants who answered each of these questions is shown in Table 6. Pairwise Wilcoxon tests were performed to group questions with a statistically similar number of responses. From this analysis, three groups emerge: question 14 with 46%, 18B with 88%, and the remaining questions with an approximately 66% answer rate. The mean number of responses differ among these groups with Holm-corrected $p < 0.005$. The differences among means for the remaining questions are not significant after Holm-correction.

Users were especially unlikely to answer $Q14$, which asked for the specific symbols in a participant's password. No other question asked for specific characters. $Q18B$ was significantly more likely to be answered than the other questions. This may be because it is a question which can be answered with a simple "No."

5.   PASSWORD COMPOSITION

This section presents our findings regarding password creation strategies, password configuration, and password entropy. It then discusses how our entropy calculations compare with those published by NIST.

---

[7]The special-character position questions ($Q17A$, $Q18A$, and $Q17B$) are an exception. For these questions, respondents only counted as refusing to answer if they explicitly selected the "I prefer not to answer" choice. This is because we suspect respondents were confused by the available answer choices.

[8]Specifically, questions 13 through 18 on survey A and 13 through 17 on survey B were considered. Question 18 on survey B was not considered because most participants answered this question, even if they declined to answer the previous five questions.

Question Summary	Number	Percent
Modified old password	243	52.4%
Created entirely new password	138	29.7%
Modified password from elsewhere	52	11.2%
Reused password from elsewhere	17	3.7%
Reused old Andrew password	11	2.4%
Modified a currently-unused password†	3	0.6%

Table 7: Responses to Question 11: "When you created your current password, which of the following did you do?". †Derived from "Other" answers.

Question Summary	Number	Percent
Word/name w. numbers/symbols added to beginning/end	204	43.4%
Based on a name	163	34.9%
Word/name w. numbers/symbols replacing some letters	79	16.8%
Based on non-English word	67	14.3%
Based on a birthday	43	9.1%
First letter of words in phrase	26	5.5%
Word/name with missing letters	20	4.3%
Based on address	11	2.3%
Based on phone number	10	2.1%

Table 8: Responses to Question 12: "Did you use any of the following strategies to create your current password (choose all that apply)?" More than one answer could be selected.

5.1 Password Creation Strategies

We asked participants if they had created a new password to meet the new requirements or modified an old one. As shown in Table 7, less than 30% of respondents created an entirely new password.

Strategies used by participants in constructing their password are shown in Table 8. Many participants used multiple strategies. For example, one participant used four strategies: based on a non-English word, numbers or symbols added to the beginning or the end, numbers or symbols substituting for letters, and missing letters. Thirty-six percent of users who reported employing any of these strategies reported using more than one.

Combining the numbers in Table 8: 210 users based their password on a word,[9] 163 based their password on a name, 56 used public information (an address, phone number, or birthday), and only 26 use a mnemonic-style password (where a password is constructed from the first letters of a phrase). Use of these strategies was not significantly related to any demographic factors, and there were no strong correlations between strategies.

5.2 Password Configuration

Table 9 summarizes length and character class information reported in our sample, and Figure 4 shows the distribution of password lengths. The mean password length was 10.5 characters, with a mode of 8.

Since the new password policy requires users to change their passwords annually, we thought some users might include a number related to the year the password was cre-

---

[9]This number combines participants who selected one of the "Based on a word" options and subtracts those participants who also selected "Based on a name."

Question Summary	Mean	σ
Password length	10.49	2.86
Number of lowercase letters	5.94	3.14
Number of uppercase letters	1.54	1.15
Number of numbers	2.70	1.88
Number of symbols	1.39	0.90

Table 9: Length and character class numbers for passwords created under the new policy.

Symbol	Freq.	Percent	Symbol	Freq.	Percent
!	86	39.6%	~	2	0.9%
@	27	12.4%	%	2	0.9%
#	20	9.2%	(	2	0.9%
*	16	7.4%	;	2	0.9%
.	13	6.0%	^	1	0.5%
$	11	5.1%	`	1	0.5%
&	10	4.6%	[	1	0.5%
-	10	4.6%	]	1	0.5%
?	8	3.7%	'	1	0.5%
<	7	3.2%	>	1	0.5%
:	6	2.8%	_	0	0%
,	5	2.3%	{	0	0%
/	5	2.3%	}	0	0%
)	4	1.8%	|	0	0%
+	4	1.8%	\	0	0%
=	3	1.4%	"	0	0%

Table 10: Frequency of occurrence for all 32 non-alphanumeric characters that count as symbols in the new password policy. Data is from the 217 users who answered this question.

ated. However, only seven of 208 users who answered Question $18B$ indicated that their password contained a number related to the year it was created. Unfortunately, we do not know how many users were aware of the annual password change requirement, because we did not want to prime participants with potentially negative information about the new policy.

Table 10 summarizes the use of symbols in participants' passwords. This table displays data for all 32 characters that are counted as symbols, according to the policy provided by the campus Information Security Office. It is notable that the three most popular choices correspond to the symbols produced by pressing $Shift$ and the numbers 1, 2, or 3 on a standard keyboard.

Many of our results in this section are presented using data from the *full disclosure* group described in Subsection 4.6. These 109 participants provided us with a nearly complete picture of their passwords. Their passwords average 10.1 characters, which is significantly shorter than the 10.7 characters of the rest of our sample. In all other ways, their password composition data is not significantly different from those of the other participants.

Character positions for the full disclosure group are shown in Table 11. Our survey also included an "Other" answer choice intended to determine the percentage of users with special characters in the middle of their password. Unfortunately, among all 470 responses, not a single one indicated "Other" for any of the character position questions. We have anecdotal evidence that participants may have misinterpreted the "Other" answer choice. Thus, we assume that participants correctly indicate the special characters in the
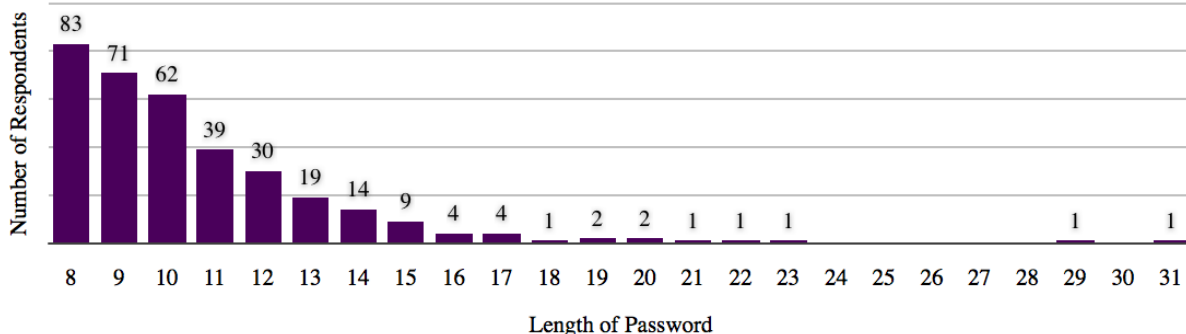
Figure 4: The lengths of passwords under the new policy.

Character	First	Second	Second from last	Last
Numbers	11.6%	7.0%	48.8%	34.9%
Symbols	2.3%	11.6%	32.6%	55.8%
Uppercase Letters	74.2%	15.2%	4.5%	10.6%

Table 11: Position percentages for the 109 participants who answered all of the questions about their password configuration. Percents may sum to above 100% due to users using multiples of the same character type.

Entropy in Length	2.68
Entropy in Numbers	
How many numbers	2.31
Where they are	1.66
‡What they are	$\log_2(10) = 3.32$
Total	**7.29**
Entropy in Symbols	
How many symbols	0.90
Where they are	1.48
What they are	3.56
Total	**5.94**
Entropy in Uppercase	
How many uppercase	1.15
Where they are	1.29
‡What they are	$1.42 \cdot 2 = 2.84$
Total	**5.28**
Entropy in Lowercase	
How many lowercase	0.00
Where they are	0.00
‡What they are	$4.91 \cdot 2 = 9.82$
Total	**9.82**
Total Entropy	**31.01**

Figure 5: This figure displays percentages for the 109 participants who answered all of the questions about their password configuration.

Table 12: Password entropy estimates, in bits, of each facet of a password. Entries that are 0 have no entropy because they are known deterministically once the other facets of a password are known. These estimates were derived from the responses of the 109 participants in the full disclosure group. ‡See text for an explanation.

first and last two positions of their password, but we make no inferences about the middle of the password.

Figure 5 shows a composite picture of the full disclosure group's first and last two characters, produced by normalizing the positional percentages between survey versions and inferring lowercase characters into the remaining spots. We used this as part of our entropy estimate for the full disclosure group's passwords.

5.3 Entropy Calculation

Entropy can be described as a measure of how hard it is to predict the value of a variable. More specifically, entropy can be considered a measure of the difficulty of guessing a password [2]. In general, the more entropy there is within a given distribution of passwords, the more difficult it is to

guess a password that was selected from that distribution. The entropy of a password distribution is important because it lower-bounds the expected number of guesses required by an attacker [12]. Passwords with larger entropy values require a larger expected number of guesses, making entropy useful as a measure of password strength.[10]

The formula used in this paper to estimate entropy was established by Claude Shannon [19]. Briefly, Shannon's formula transforms a distribution into an entropy estimate.[11]

---

[10]Using an optimal strategy, $E[G] \geq 2^{H-2} + 1$, where $E[G]$ is the expected number of guesses and H is the entropy in bits [12].

[11]For each possible value x of a variable, the probability of that value occurring is $p(x)$. The entropy is then calculated as $H = -\sum_x [p(x) \lg p(x)]$. It is typically measured in bits.

Because Shannon's formula for entropy is additive, we are able to calculate entropy for a distribution of passwords as a whole by summing the entropy derived from individual facets of those passwords. We can separately estimate the entropy derived from password length, character placement, number of each character type in the password, and the content of each character; and then combine these to form an estimate of the total password entropy.

An example will clarify the calculation; let us consider the entropy derived from the length of a password. The probability of a password having a specific length is determined by dividing the number of passwords that have that length by the total number of passwords in a distribution. Since 28% of respondents in the full disclosure group had passwords of length 8, the probability of this length is 0.28. Shannon's formula is then applied to the probabilities for all lengths, which we calculate from our survey data from the full disclosure group. This calculation gives an entropy of 2.68 bits for password length, indicating that password length contributes this amount to the total entropy of passwords under our password policy.

The entropy contributed by many facets of passwords, such as character placement and number of each character, can similarly be computed using our survey data. We also collected data on which symbols were used by specifically asking participants to list the symbols in their passwords. However, we did not collect similar data for numbers or letters in passwords. Those facets for which entropy could not be computed are denoted with a ‡ in Table 12. One of them is "what the numbers are," which we estimate to be equal to the entropy of a single random digit, although participants actually used an average of 2.45 digits per password. A similar issue occurs with lowercase and uppercase letters. Since we do not have exact data on what these are, we use the NIST estimate of 2 bits per letter for their entropy [2]. The numbers 1.42 and 4.91 in Table 12 represent the average number of uppercase and lowercase letters, respectively, found in the full disclosure group's passwords. Finally, entries in Table 12 that are 0 have no entropy because they are known deterministically once the other facets of a password are known.

In this way, we can calculate an estimate of the entropy of the different facets of the CMU password space. By summing these values, we derive an entropy estimate of the passwords as a whole. The components of this summation are shown in Table 12. Our estimated entropy for CMU passwords is about 31 bits.

This estimate may be an overestimate because it does not account for correlations between facets. To illustrate, consider the placement of symbols in a password. If certain symbols are only found in certain positions, the probabilities associated with symbol placement will be dependent on symbol content. This decreases the total entropy.[12] Since we do not have data at this level, we are forced to ignore such correlations. On the other hand, Shannon's entropy formula produces an underestimate of the true entropy when applied to a small random sample of a population [13]. Further, our entropy calculation does not consider the fact that the CMU password policy institutes a dictionary check, because we do not have data on how this check affected entropy. This is explained in more detail in Section 5.5.3.

---

[12]As given by Shannon, the joint entropy $H(X, Y) \leq H(X) + H(Y)$ where $H(\cdot)$ is the entropy function [19].

Question Summary		Estimated Entropy in Bits
$Q14.$	What symbols in password?	4.95†
$Q15A.$	How many lowercase letters?	3.43
$Q13.$	Password Length?	2.97
$Q16B.$	How many numbers?	2.52
$Q17A.$	In which positions are numbers?	1.99
$Q15B.$	How many symbols?	1.87
$Q17B.$	In which positions are uppercase letters?	1.61
$Q16A.$	How many uppercase letters?	1.38
$Q15B.$	How many symbols?	1.11
$Q18B.$	Contains number related to year created?	0.21

Table 13: The estimated entropy per question. This table shows the amount of information revealed by a participant answering each of these questions. †This is a cumulative score based on 3.56 average bits per symbol and 1.39 average number of symbols revealed ($3.56 \cdot 1.39 = 4.95$). The proportion of participants answering each question is found in Table 6.

5.4 Entropy and Refusal to Answer

Our results indicate that participants were less likely to answer questions that divulge more about their passwords. Table 13 shows the amount of information derived from the answers to each survey question, as determined by calculating Shannon entropy over its given responses. The results given in Table 13 differ slightly from those in Table 12 because they are over all responses, not just those from the full disclosure group.

Participants' refusal to answer a question, as shown in Table 6, was strongly correlated with the amount of information disclosed by that question ($r = 0.74$). This suggests that participants intuitively know which questions uncover more information about their passwords. In particular, as mentioned in Section 4.6, participants were especially unlikely to answer $Q14$ (what symbols), which reveals the most information about their passwords; and especially likely to answer $Q18B$ (contains year), which reveals the least information about their passwords.

5.5 Comparison to NIST Estimate

As mentioned in Section 2.1, the change to the CMU password policy was based on NIST guidelines that provide a heuristic for estimating the entropy of user passwords [2]. In this section, we present some of the NIST assumptions and compare them with our own results.

5.5.1 Password Length

The NIST heuristic assumes passwords will be exactly the minimum length. However, as shown in Figure 4, only 24% of respondents (83/343) reported a password of length 8. If an attacker assumes a password is of minimum length, he or she only has a 24% chance of successfully cracking a user's password after exhausting the entire 8-character password space. We estimate that length contributes 2.68 bits of entropy to passwords under the CMU password policy.

5.5.2 Special Characters

The NIST guidelines make the following assertion about special characters, which include uppercase letters, numbers, and symbols:

> ...the assumption here is that users will choose passwords that are almost entirely lower case let-

ters, unless forced to do otherwise, and [rules] that force them to include capital letters or non-alphabetic characters will generally be satisfied in the simplest and most predictable manner, often by putting a capital letter at the start ... and punctuation or special characters at the end...

The NIST heuristic awards a flat 6 bits of entropy for the inclusion of uppercase and non-alphabetic characters and 2 bits of entropy for each character, regardless of character type. Applying this formula to the CMU password policy yields an entropy contribution of 12 bits from the special characters, if we assume a password of eight characters including three special characters: one uppercase letter, one number and one symbol ($6 + 3 * 2 = 12$).

In contrast, our results find that much of the entropy contributed by uppercase and non-alphabetic characters comes from users exceeding the minimum requirements: using more numbers than necessary and varying the positions of special characters. Our participants frequently chose passwords that exceeded the minimum requirements of the policy. Only 31% (49/156) reported having a single number; 73% (115/158) and 76% (111/146) reported having only one uppercase letter or symbol, respectively. In addition, many respondents reported having uppercase letters at the end of their passwords, or numbers or symbols at the beginning.[13] We estimate the cumulative entropy of these character types per password to be 18.51 bits. This is found by summing the entropies contributed by special characters in Table 12.

5.5.3 Dictionary Checks

Forty-five percent of our participants based their password on a word, despite the fact that the CMU password policy includes a dictionary check. This dictionary check operates by removing all non-alphabetic characters from a password and checking the remaining string against a dictionary. Thus even if a password does contain a dictionary word, as long as there are additional letters before, after, or within the word, it satisfies the requirement. Concatenation of multiple words is also allowed. This checking algorithm is consistent with NIST's conception of a dictionary check, which in the NIST heuristic contributes a bonus of 6 bits to a password's entropy.

Although we expect this check may increase the entropy of passwords as a whole, we ignore the effect of this check in our estimate. Validating it requires complete knowledge of a user's password, and our survey does not have this level of detail. What we do know is that, despite this check, almost half of our participants claimed to have a password based on a word.

5.5.4 Defining Requirements

Although our calculations and the heuristics of NIST approach the problem of defining entropy for a given password policy quite differently, both depict the CMU password policy as having a per-password entropy of roughly 30 bits.

However, there are other password policies which could generate this level of entropy, beyond just the policy requirements set forth at CMU. Using the NIST heuristic, a randomly-assigned 5-character password has an entropy of

33 bits. A 14-character user-chosen password with no special character requirements would also have about 30 bits of entropy, using the NIST heuristic. Though previous work has found that long, passphrase-style passwords lead to more typographic mistakes and user dissatisfaction [8], the results of our survey suggest that some users prefer them. As seen in Figure 4, 11% of our respondents currently have passwords that are 14 characters or longer. These users do not need the additional restrictions of a strict password policy to have a sufficiently strong password. Other users might favor randomly-assigned, shorter passwords. If all of these policies have sufficient entropy, it may be acceptable to allow users to choose the policy that fits them best. This would maintain security while improving usability.

6. DISCUSSION

This work presents several new insights regarding user attitude and behavior under strict password policies. The highlights are presented below.

Users find new requirements annoying but believe they provide security. Our survey was conducted on a population shortly after a required password policy transition from a less-constrained policy to a stricter one. Users were annoyed by this change. However, they did feel more secure under the new policy.

Some users struggle to comply with new password requirements. Most users created their new password in a single attempt, and believed they would be able to login in one try. However, 19% of users reported already forgetting their new passwords. These users seem to have struggled with the policy change. They required significantly more attempts to create their new passwords, believed that logging in would require more attempts, were more annoyed, found creating the new password less fun, and were more likely to write their password down. Over 10% of these users went to the help desk because they forgot their passwords.

Users are more likely to share and reuse their passwords than to write them down. Much has been made of users writing down passwords. However, we found fewer Andrew users writing down their old or new passwords than would be expected based on previous work [16, 24]. On the other hand, over a quarter of our respondents reported they have shared a new or old Andrew password, and over three quarters of users reuse passwords. Despite the fact that some experts advocate writing passwords down as a mechanism to cope with numerous passwords [18], reusing passwords seems to be much more prevalent than writing them down.

Users tend to modify old passwords to create new ones. About half our respondents reported modifying their old password to create their new one. Others modified or reused a password for another account. This suggests that many users avoid creating completely new passwords when forced to change. Since the new passwords were required to include character classes not previously required, some users may have added additional characters to their previous password. This may explain why the average length of new passwords was over 2 characters longer than required by policy.

Users are more likely to share their passwords over time. Around 25% of users reported having shared their old password with at least one person. This percentage is more than twice the percentage of users who have shared new passwords (12%). This behavior may be associated with

---

[13]27% and 18% of respondents had numbers or symbols in the first two characters of their passwords, respectively; and 22% had an uppercase letter in one of the last two positions.

the fact that, as time passes, users face situations where they need to share their passwords, such as when they need someone else to help them access their accounts when out of the office. This suggests that a password policy requiring a periodic change of passwords could help to protect users' passwords. However, the impact of such a policy on password composition, and other aspects of user behavior, should also be considered.

Use of dictionary words and names are still the most common strategies to create passwords. Nearly 80% of users based their password on a word or name, with special characters added to the beginning or end. This is despite the new policy implementing a basic check for dictionary words.

Our results reveal flaws in NIST's assumptions. NIST bases its per-password entropy estimates on several assumptions that are inconsistent with our findings [2]. They assume users will create passwords of the minimum required length, but our results show an average length more than two characters above the minimum. NIST also assumes users will have the minimum number of special characters, but our participants frequently indicated using more. Over two-thirds of users who responded said they used more than the one required number. It would be useful to examine larger sets of passwords created under a variety of password policies to provide empirical data to improve the NIST guidelines.

7. ACKNOWLEDGMENTS

8. REFERENCES

[1] M. Bishop and D. V.Klein. Improving system security via proactive password checking. *Computers & Security*, 14(3):233–249, 1995.

[2] W. E. Burr, D. F. Dodson, and W. T. Polk. Electronic authentication guideline. Technical report, National Institute of Standards and Technology, 2006.

[3] D. Florencio and C. Herley. A large-scale study of web password habits. In *International conference on World Wide Web*, page 666, 2007.

[4] E. F. Gehringer. Choosing passwords: security and human factors. *International Symposium on Technology and Society, 2002*, pages 369–373, 2002.

[5] D. Hart. Attitudes and practices of students towards password security. *Journal of Computing Sciences in Colleges*, 23(5):169–174, 2008.

[6] C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *New Security Paradigms Workshop*, pages 133–144, 2009.

[7] P. Inglesant and M. A. Sasse. The true cost of unusable password policies: password use in the wild. In *ACM Conference on Human Factors in Computing Systems 2010*, pages 383–392, 2010.

[8] M. Keith, B. Shao, and P. J. Steinbart. The usability of passphrases for authentication: An empirical field study. *International journal of human-computer studies*, 65(1):17–28, 2007.

[9] S. Komanduri and D. R. Hutchings. Order and entropy in picture passwords. In *Graphics Interface*, pages 115–122, 2008.

[10] C. Kuo, S. Romanosky, and L. F. Cranor. Human selection of mnemonic phrase-based passwords. In *Symposium on Usable Privacy and Security*, pages 67–78, 2006.

[11] J. Leyden. Office workers give away passwords for a cheap pen. *The Register*, 2003.

[12] J. L. Massey. Guessing and entropy. In *IEEE International Symposium on Information Theory*, page 204, 1994.

[13] G. Miller. Note on the bias of information estimates. *Information Theory in Psychology: Problems and Methods*, pages 95–100, 1955.

[14] R. W. Proctor, M.-C. Lien, K.-P. L. Vu, E. E. Schultz, and G. Salvendy. Improving computer security for authentication of users: Influence of proactive password restrictions. *Behavior Research Methods, Instruments, & Computers*, 34(2):163–169, 2002.

[15] RSA. Rsa security survey reveals multiple passwords creating security risks and end user frustration. `http://www.rsa.com/press_release.aspx?id=6095`, September 2010.

[16] SafeNet. 2004 annual password survey results. *SafeNet*, 2005.

[17] M. A. Sasse, S. Brostoff, and D. Weirich. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19(3):122–131, 2001.

[18] B. Schneier. Write down your password. `http://www.schneier.com/blog/archives/2005/06/write_down_your.html`, June 2005.

[19] C. E. Shannon. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(1), 1949.

[20] R. Shay and E. Bertino. A comprehensive simulation tool for the analysis of password policies. *International Journal of Information Security*, 8(4):275–289, 2009.

[21] R. Shay, A. Bhargav-Spantzel, and E. Bertino. Password policy simulation and analysis. In *ACM workshop on Digital identity management*, pages 1–10, 2007.

[22] W. C. Summers and E. Bosworth. Password policy: the good, the bad, and the ugly. In *Winter international synposium on Information and communication technologies*, pages 1–6, 2004.

[23] K.-P. L. Vu, R. W. Proctor, A. Bhargav-Spantzel, B.-L. B. Tai, and J. Cook. Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, 65(8):744–757, 2007.

[24] M. Zviran and W. J. Haga. Password security: an empirical study. *Journal of Management Information Systems*, 15(4):161–185, 1999.

APPENDIX

A. SURVEY

ANDREW PASSWORD CHANGE SURVEY

Please only fill out this survey if you have an Andrew account and have changed your password to comply with the new password rules announced in December 2009.

The information we are collecting is anonymous. We aren't recording your name or your ID. We will be unable to tie the information collected here to any particular Andrew user.

We aren't asking for your password. Please do not tell anyone your password.

This survey is being conducted by Carnegie Mellon students and faculty. For more information, please contact the Principal Investigator: Lorrie Cranor <lorrie@cmu.edu>. If you have questions pertaining to your rights as a research participant, or to report objections to this study, you should contact the Research Regulatory Compliance Office at Carnegie Mellon University. Email: irb-review@andrew.cmu.edu. Phone: 412-268-1901 or 412-268-5460. The Carnegie Mellon University Institutional Review Board (IRB) has approved the use of human participants for this study.

1. What is your role at CMU: ___ Student ___ Faculty ___ Staff ___ Other

2. What is your gender? ___ Male ___ Female

3. How old are you? _____

4. Are you majoring in or do you have a degree or job in computer science, computer engineering, information technology, or a related field? ___ Yes ___ No

5. When did you change your password to comply with the new policy?
   ___ I have not changed my password to comply with the new policy yet
   ___ The same day I got the password change email
   ___ Not the same day, but before a second password change email
   ___ After I got multiple password change emails
   ___ I'm not sure

6. If you tried to login to your Andrew account right now, how many attempts do you think it would take? _____

7. To how many people have you given your current password? _____

8. To how many people have you given your old password? _____

9. Have you ever forgotten your current password? ___ Yes ___ No

10. If yes, how did you recover it?
    ___ I remembered it later   ___ I told it to someone else so I asked them
    ___ I had written it down so I was able to look it up ___ I went to the help desk
    ___ It is remembered by my browser or email client   ___ I never recovered it
    ___ Other _____

11. When you created your current password, which of the following did you do?
    ___ I reused my old Andrew password
    ___ I modified my old Andrew password to meet the new requirements
    ___ I reused a password I was already using for a different account
    ___ I modified a password I was already using for a different account
    ___ I created an entirely new password
    ___ Other _____

12. Did you use any of the following strategies to create your current password (choose all that apply)?
    ___ Password based on the first letter of each word in a phrase
    ___ Based on the name of someone or something
    ___ Based on a word or name with numbers / symbols added to beginning or end
    ___ Based on a word or name with numbers and symbols substituting for some of the letters (e.g. '@' instead of 'a')
    ___ Based on a word or name with letters missing
    ___ Based on a word in a language other than English   ___ Based on an address
    ___ Based on a phone number   ___ Based on a birthday

13. How long is your current password (total number of characters)? _____   __I prefer not to answer

14. What symbols (characters other than letters and numbers) are in your password? _____   __I prefer not to answer

15. How many lower-case letters are in your current password? ____   __I prefer not to answer

16. How many upper-case letters are in your current password? ____   __I prefer not to answer

17. In which positions in your password are the numbers?   __ I prefer not to answer
    __ First   __ Second   __ Second from last   __ Last   __ Other

18. In which positions in your password are the symbols?   __ I prefer not to answer
    __ First   __ Second   __ Second from last   __ Last   __ Other

19. How many tries did it take to create a password the system accepted? _____

20. Have you written down your current password?
    __ No   __ Yes, on paper   __ Yes, electronically (stored in computer, phone, etc.)   __ Other _____

    If you wrote down your current password how is it protected (choose all that apply)?
    __ I do not protect it   __ I stored it in an encrypted file
    __ I hid it   __ I stored it on a computer or device protected with another password
    __ I locked up the paper
    __ I always keep the password with me
    __ I wrote down a reminder instead of the actual password
    __ Other _____

21. Have you written down your old password?
    __ No   __ Yes, on paper   __ Yes, electronically (stored in computer, phone, etc.)   __ Other _____

    If you wrote down your old password how is it protected (choose all that apply)?
    __ I do not protect it   __ I stored it in an encrypted file
    __ I hid it   __ I stored it on a computer or device protected with another password
    __ I locked up the paper
    __ I always keep the password with me
    __ I wrote down a reminder instead of the actual password
    __ Other _____

22. Do you have a set of passwords you reuse in different places?   __Yes   __No

23. Do you have a password that you use for different accounts with a slight modification for each account?
    __Yes   __No

24. With the new password requirements, my Andrew account is more secure.
    __ Strongly agree   __ Agree   __ Neutral   __ Disagree   __ Strongly disagree

25. Creating a password that meets the new requirements was annoying.
    __ Strongly agree   __ Agree   __ Neutral   __ Disagree   __ Strongly disagree

26. Creating a password that meets the new requirements was difficult.
    __ Strongly agree   __ Agree   __ Neutral   __ Disagree   __ Strongly disagree

27. Creating a password that meets the new requirements was fun.
    __ Strongly agree   __ Agree   __ Neutral   __ Disagree   __ Strongly disagree

28. Any added protection provided by the new password is worth the added effort of creating/remembering/using it.
    __ Strongly agree   __ Agree   __ Neutral   __ Disagree   __ Strongly disagree

29. I would like Andrew to go back to the old password policy.
    __ Strongly agree   __ Agree   __ Neutral   __ Disagree   __ Strongly disagree

A

13. How long is your current password (total number of characters)? _____   __I prefer not to answer

14. What symbols (characters other than letters and numbers) are in your password? _____   __I prefer not to answer

15. How many symbols (characters other than letters and numbers) are in your current password? ____
                                                                                          __ I prefer not to answer

16. How many numbers are in your current password? ____   __I prefer not to answer

17. In which positions in your password are the capital letters?   __ I prefer not to answer
     __ First   __ Second   __ Second from last   __ Last   __ Other

18. Does your password contain a number related to the year it was created?
     __ Yes   __ No   __ I prefer not to answer

19. How many tries did it take to create a password the system accepted? _____

20. Have you written down your current password?
     __ No   __ Yes, on paper   __ Yes, electronically (stored in computer, phone, etc.)   __ Other _____

     If you wrote down your current password how is it protected (choose all that apply)?
     __ I do not protect it   __ I stored it in an encrypted file
     __ I hid it   __ I stored it on a computer or device protected with another password
     __ I locked up the paper
     __ I always keep the password with me
     __ I wrote down a reminder instead of the actual password
     __ Other _____

21. Have you written down your old password?
     __ No   __ Yes, on paper   __ Yes, electronically (stored in computer, phone, etc.)   __ Other _____

     If you wrote down your old password how is it protected (choose all that apply)?
     __ I do not protect it   __ I stored it in an encrypted file
     __ I hid it   __ I stored it on a computer or device protected with another password
     __ I locked up the paper
     __ I always keep the password with me
     __ I wrote down a reminder instead of the actual password
     __ Other _____

22. Do you have a set of passwords you reuse in different places?   __Yes   __No

23. Do you have a password that you use for different accounts with a slight modification for each account?
     __Yes   __No

24. With the new password requirements, my Andrew account is more secure.
     __ Strongly agree   __ Agree   __ Neutral   __ Disagree   __ Strongly disagree

25. Creating a password that meets the new requirements was annoying.
     __ Strongly agree   __ Agree   __ Neutral   __ Disagree   __ Strongly disagree

26. Creating a password that meets the new requirements was easy.
     __ Strongly agree   __ Agree   __ Neutral   __ Disagree   __ Strongly disagree

27. Creating a password that meets the new requirements was fun.
     __ Strongly agree   __ Agree   __ Neutral   __ Disagree   __ Strongly disagree

28. Any added protection provided by the new password is worth the added effort of creating/remembering/using it.
     __ Strongly agree   __ Agree   __ Neutral   __ Disagree   __ Strongly disagree

29. I would like Andrew to go back to the old password policy.
     __ Strongly agree   __ Agree   __ Neutral   __ Disagree   __ Strongly disagree

B

B. SURVEY RESPONSES

This survey is filled in with the responses we received.

ANDREW PASSWORD CHANGE SURVEY

1. What is your role at CMU: **413** Student   **10** Faculty   **41** Staff   **6** Other

2. What is your gender?   **228** Male   **241** Female   Blanks: **1**

3. How old are you?
   Less than 22: **280**
   Equal to or more than 22: **185**
   Blanks:**5**

4. Are you majoring in or do you have a degree or job in computer science, computer engineering, information technology, or a related field?   **162** Yes   **301** No   Blanks:**7**

5. When did you change your password to comply with the new policy?
   0 I have not changed my password to comply with the new policy yet
   94 The same day I got the password change email
   149 Not the same day, but before a second password change email
   215 After I got multiple password change emails
   11 I'm not sure
   Blanks: **1**

6. If you tried to login to your Andrew account right now, how many attempts do you think it would take?
   1 try:**356**
   2 tries: **77**
   3 tries: **15**
   Five tries:**1**
   Blanks: **21**

7. To how many people have you given your current password?
   Zero:**397**
   One: **51**
   Two: **6**
   Three:**1**
   Blanks: **15**

8. To how many people have you given your old password?
   Zero:**332**
   One:**78**
   Two:**24**
   Three:**9**
   Four:**3**
   Five:**3**
   More than five: **4**
   Blanks:**17**

9. Have you ever forgotten your current password? **87** Yes   **375** No   Blanks:**8**

10. If yes, how did you recover it?
    55 I remembered it later   __ I told it to someone else so I asked them
    21 I had written it down so I was able to look it up   **10** I went to the help desk
    1 It is remembered by my browser or email client   **1** I never recovered it
    5 Other

11. When you created your current password, which of the following did you do?
    11 I reused my old Andrew password
    243 I modified my old Andrew password to meet the new requirements
    17 I reused a password I was already using for a different account
    52 I modified a password I was already using for a different account
    138 I created an entirely new password
    4 Other
    Blanks: **5**

12. Did you use any of the following strategies to create your current password (choose all that apply)?
    26 Password based on the first letter of each word in a phrase
    163 Based on the name of someone or something
    204 Based on a word or name with numbers / symbols added to beginning or end
    79 Based on a word or name with numbers and symbols substituting for some of the letters (e.g. '@' instead of 'a')
    20 Based on a word or name with letters missing
    67 Based on a word in a language other than English   **11** Based on an address
    10 Based on a phone number   **43** Based on a birthday

13. How long is your current password (total number of characters)? **10.5**   **127** I prefer not to answer

14. What symbols (characters other than letters and numbers) are in your password?
    253 I prefer not to answer (**See details in table 10)**

19. How many tries did it take to create a password the system accepted? **1.77**   Blanks:**39**

20. Have you written down your current password?
    394 No   **40** Yes, on paper   **23** Yes, electronically (stored in computer, phone, etc.)   **9** Other

    If you wrote down your current password how is it protected (choose all that apply)?
    17 I do not protect it   **6** I stored it in an encrypted file
    9 I hid it   **7** I stored it on a computer or device protected with another password
    5 I locked up the paper
    7 I always keep the password with me
    4 I wrote down a reminder instead of the actual password   __ Other

21. Have you written down your old password?
    402 No   **35** Yes, on paper   **21** Yes, electronically (stored in computer, phone, etc.)   **6** Other

    If you wrote down your old password how is it protected (choose all that apply)?
    8 I do not protect it   **6** I stored it in an encrypted file
    12 I hid it   **11** I stored it on a computer or device protected with another password
    2 I locked up the paper
    3 I always keep the password with me
    7 I wrote down a reminder instead of the actual password   __ Other

22. Do you have a set of passwords you reuse in different places?   **381** Yes   **75** No   Blanks: **14**

23. Do you have a password that you use for different accounts with a slight modification for each account?
    281 Yes   **173** No   Blanks:**16**

24. With the new password requirements, my Andrew account is more secure.
    69 Strongly agree   **180** Agree   **153** Neutral   **45** Disagree   **7** Strongly disagree
    Blanks:**16**

25. Creating a password that meets the new requirements was annoying.
    115 Strongly agree   **176** Agree   **104** Neutral   **51** Disagree   **14** Strongly disagree
    Blanks: **10**

27. Creating a password that meets the new requirements was fun.
    8 Strongly agree **22** Agree   **141** Neutral   **150** Disagree   **139** Strongly disagree
    Blanks:**10**

28. Any added protection provided by the new password is worth the added effort of creating/remembering/using it.
    54 Strongly agree   **165** Agree   **169** Neutral   **55** Disagree   **15** Strongly disagree
    Blanks:**12**

29. I would like Andrew to go back to the old password policy.
    24 Strongly agree   **45** Agree   **249** Neutral   **105** Disagree   **37** Strongly disagree
    Blanks: **10**

Exclusive questions for survey A

15. How many lower-case letters are in your current password? **5.94**   **83** I prefer not to answer

16. How many upper-case letters are in your current password? **1.54**   **76** I prefer not to answer

17. In which positions in your password are the numbers?   **83** I prefer not to answer
    14 First   **4** Second   **28** Second from last   **47** Last   ___ Other

18. In which positions in your password are the symbols?   **79** I prefer not to answer
    7 First   **12** Second   **24** Second from last   **61** Last   ___ Other

26. Creating a password that meets the new requirements was difficult.
    17 Strongly agree   **49** Agree   **60** Neutral   **77** Disagree   **25** Strongly disagree
    Blanks:**7**

Exclusive questions for survey B

15. How many symbols (characters other than letters and numbers) are in your current password? **1.39**
    90 I prefer not to answer

16. How many numbers are in your current password? **2.70**
    80 I prefer not to answer

17. In which positions in your password are the capital letters?   **80** I prefer not to answer
    91 First   **11** Second   **5** Second from last   **9** Last   0 Other

18. Does your password contain a number related to the year it was created?
    7 Yes   **201** No   **28** I prefer not to answer

26. Creating a password that meets the new requirements was easy.
    29 Strongly agree   **81** Agree   **59** Neutral   **55** Disagree   **7** Strongly disagree
    Blanks: **5**