Password Management Strategies for Online Accounts

Shirley Gaw
Department of Computer Science
Princeton University
Princeton, NJ USA
sgaw@cs.princeton.edu

Edward W. Felten
Center for Information Technology Policy
Wilson School of Public and International Affairs
Department of Computer Science
Princeton University
Princeton, NJ USA
felten@cs.princeton.edu

ABSTRACT

Given the widespread use of password authentication in online correspondence, subscription services, and shopping, there is growing concern about identity theft. When people reuse their passwords across multiple accounts, they increase their vulnerability; compromising one password can help an attacker take over several accounts. Our study of 49 undergraduates quantifies how many passwords they had and how often they reused these passwords. The majority of users had three or fewer passwords and passwords were reused twice. Furthermore, over time, password reuse rates increased because people accumulated more accounts but did not create more passwords. Users justified their habits. While they wanted to protect financial data and personal communication, reusing passwords made passwords easier to manage. Users visualized threats from human attackers, particularly viewing those close to them as the most motivated and able attackers; however, participants did not separate the human attackers from their potentially automated tools. They sometimes failed to realize that personalized passwords such as phone numbers can be cracked given a large enough dictionary and enough tries. We discuss how current systems support poor password practices. We also present potential changes in website authentication systems and password managers.

Categories and Subject Descriptors

H.5.2 [**User Interfaces**]: Evaluation/methodology; K.6.5 [**Security and Protection**]: Authentication

General Terms

password management, user behavior, password reuse

Keywords

security, password, survey, user behavior

1. INTRODUCTION

For password authentication systems, users often *are* the enemy. Schneier writes, "the problem is that the average user can't and won't even try to remember complex enough passwords to prevent dictionary attacks. As bad as passwords are, users will go out of the way to make it worse. If you ask them to choose a password, they'll choose a lousy one. If you force them to choose a good one, they'll write it on a Post-it and change it back to the password they changed it from the last month. And they'll choose the same password for multiple applications." [22] In short, poor password practices undermine the system.

Many projects focus on developing new technology around these poor practices without studying them. In contrast, this paper broadly looks at password practices, quantifying password reuse and also surveying the contributing factors to this reuse. We not only consider how users justify their poor practices but also study what encourages them to do better. We link these practices password management tools and discuss ways current technology supports poor practices. We also demonstrate users are ill-informed about dictionary attacks from responses to a survey of what constitutes strong passwords and who could compromise passwords.

Our password study focuses on online accounts. Website authentication scales up a user's password management problem. For real world interactions, users can leverage physical context: they stand at an ATM, they hold a cell phone, or they sit in front of their desktop. For online accounts, users are at the same machine but access many different accounts. Second, real world interactions also have more regularity: people may use their voicemail password or their building entry codes almost daily. Online interactions may be more sporadic, where users visit a specific site rarely. Altogether, these issues and the proliferation of website logins aggravate the password management problem, particularly encouraging password reuse [2, 11].

Technical solutions for online password management can improve practice and without significantly changing user beavior. This is in contrast to alternatives for traditional authentication systems. These alternatives might rely on the user having a particular device such as a cell phone or a physical token such as a smart card. When users access website accounts, they already have their hands on a computer. We can develop systems at the application level or at the browsers specifically instead of at the device level.

A newly developed system should incorporate the needs of users, but few have studied users' work practices in this domain. As Preece states, we must take this step to "approach it by understanding the characteristics and capabilities of the users, what they are trying to achieve, how they achieve it currently, and whether they would achieve their

Symposium On Usable Privacy and Security (SOUPS) 2006, July 12-14, 2006, Pittsburgh, PA, USA.

goals more effectively if they were supported differently." [17]

In this paper, we present a survey of how users manage passwords for online accounts. With this background on what users do, we can develop supportive technologies for password management. In our study with 49 undergraduates, we measure the extent of password reuse and examine users' justifications of this practice. We ask about current management strategies and use data from failed login attempts to understand where users have problems with password authentication. We also investigate users' models of attacks and attackers, which provide context to their security precautions. The large scope of this work helps us understand real users' practices along with the environment and culture that leads to these practices.

2. RELATED WORK

As mentioned in the introduction, many projects try to overcome poor password practices. For instance, several researchers have suggested using graphical passwords, whether they use doodles [10], a series of random art images [7] or people's faces [3], or points within an image [25]. The premise with these systems is that images are easier for people to recognize or recall than text. Additionally, these systems may afford selection of stronger passwords [12] than poor text passwords that are easily cracked [14, 15]. In contrast, Yan et al. and Bunnell et al. have focused on text passwords, looking at recall rates for different methods to generate and associate these passwords [26, 6].

Others have looked at tools for users to manage their passwords, particularly password hashing systems. Yee discusses several password hashing systems, which can use a master password on a second identifier (such as a website URL) to generate unique passwords across different websites [27]. Often these tools try to add convenience by hiding their functions from the user. Both LPWA and PwdHash automatically substitute or fill in passwords based on specific user input [9, 20], while Site Password [13] and a remote version of PwdHash display the generated password for the user. Browser features such as Internet Explorer's AutoComplete and Firefox's Saved Passwords similarly automate filling in passwords without displaying clear text to the user. These functions then relieve the user's burden to memorize several passwords.

Researchers have also conducted empirical studies of password use and management. Petrie collected passwords from 1,200 employees in the United Kingdom. The author concluded that people tended to pick passwords that represent themselves, a person's "password has to sum up the very essence of their being in one word" [16]. In our study, we further asked participants who they thought would be most able to attack their passwords, which indicated whether participants believed a personal relationship presents an advantage for compromising passwords.

Several papers rely on interview data to understand how users manage their passwords. Adams and Sasse conclude that users lack motivation and do not understand of password policies [1]. Weirich and Sasse further study attitudes toward strengthening password management [23, 24]. Their studies indicates users, to some degree, deny their vulnerability. In our study, we asked participants to evaluate the likelihood of attack from different groups of people. We wondered if the problem lies in a lack of understanding of how to strengthen password management and also studied how users justify subverting password policies.

There have been few papers that empirically quantify how many passwords people have. Dhamija and Perrig used interview data from 30 people to estimate that participants had one to seven unique passwords for ten to fifty websites [7]. Sasse et al. investigated several aspects of password use. They reported that the 144 employees surveyed had an average of 16 passwords, but this was not limited to online activities [21]. Two other studies have based estimations of people's passwords through surveys. Brown et al. surveyed college students and asked how many passwords they had. Students had an average of 8.18 password uses with 4.45 unique passwords ($N = 218$) [4]. Riley also used a survey to focus on online accounts. Her results similarly indicated college and graduate students had an average of 8.5 accounts with an passwords ($SD = 2.028$, $N = 328$) [19]. In contrast to the above papers, our study collected password information based on login attempts to websites before asking users to estimate how many passwords they had; that is, rather than asking people to just estimate how many passwords they had, they were first asked to login to websites and then count how many passwords they used.

3. OVERVIEW OF STUDY

We broadly studied password practices, focusing on real users password reuse and the technology designs that encouraged (or discouraged) these practices. Our study was part laboratory exercise and part survey. Participants who completed the two sessions of the study were compensated with $10 USD. Almost all participants were Princeton University undergraduates, with the exception of one graduate student and two people unaffiliated with the university. Sections 5 and 6.1 present results from the first session, where students completed an online questionnaire (58 participants: 18 males, 40 females). Sections 4 and 6.2 present results from the second session, where students came into the laboratory. Only 49 of the original participants completed the second session (33 females, 16 males).

4. QUANTIFYING PASSWORD REUSE

How many online accounts do people have? BugMeNot.com claims to have accounts for at least 107,116 free websites that use password authentication [5]. While this *collection* is huge, *individual users* have far fewer website accounts. Our survey asked participants to quantify how many website accounts they had and how many passwords they used across these accounts.

We were interested in having participants recall the websites where they had accounts and recall their login information. Unfortunately, people are unlikely to recall more than a handful of websites they use. They also need to check their login information online to be sure they are correct. Instead, we could have provided lists of sites, had participants select the websites where they had accounts, and then had them log in to those accounts. If we provided lists of websites, however, we would miss any website the participants used but we neglected to include. We finally combined both approaches and developed a login task where participants make *one pass* at recording their online account information with pre-made lists and then a *second pass* with open-ended queries.

4.1 Method

Participants. We requested participants bring "anything you use to help you remember your passwords (password lists, daily planners or notebooks, digital assistants, copies of bank or travel statements, copies of items in your Internet browser cache, etc.)" Of the 49 participants, six brought aids (e.g., a travel statement, a daily planner, and paper password lists). Twenty-six participants used their own laptops in the study while the remaining 23 were provided with a Firefox web browser on a Dell PC.

Procedure. Participants were told the study would ask them to indicate which websites they used, login to these websites, and write down their passwords. Using provided writing materials and a manila folder, they were instructed to track their passwords and to hide their passwords from the experimenters. They were also told that they could access e-mail accounts to help them in the experiment.

Participants estimated their use of websites and passwords in two passes. In the *first pass*, participants were directed to a CGI script that presented the names of 139 websites grouped into 12 categories (news, travel, finance, shopping, communication, computers & Internet, entertainment, services, reference, sports, journals & magazines, and clothes shopping).[1] Each of the websites used login authentication, although some were login services. This created overlap; for example, at the time of the study, Expedia.com had their own authentication system but also supported Microsoft Passport. In each category, participants indicated if they "have an account on the following websites." In cases where a participant was unsure if they had account, the experimenters instructed them to overestimate which websites they used. Participants also included accounts that were shared with family members. For each site where a participant indicated they had an account, they were presented with a webpage that instructed them to log in to the website using a provided link. Clicking on the link popped open a new browser window. They were told "you have 90 seconds to try to login to the website. When you have finished, close the [website] window to return to this page." If participants spent longer than 90 seconds without responding to the CGI script, the webpage refreshed and recorded an unsuccessful login. For each site, participants were asked if they were "able to login to the website on your first attempt" although the experimenters observed participants attempting to login more than once. For successful logins, participants wrote down their passwords on a paper list. For unsuccessful logins, participants explained why they were unsuccessful at logging into the site.

After finishing all logins, participants self-reported summary statistics on the number of passwords they used in the experiment. Participants reported counts for five measures: the number of passwords collected in the experiment, the number of unique passwords, the size of classes of similar passwords, the number of password repetitions, and the number of passwords with related meanings.

In the *second pass*, participants listed sites that they used but were overlooked in the first pass. This was added to measures of number of online accounts. Participants were told to "write down all of your other passwords that you can recall" and re-report their summary statistics. They were instructed to use any tools "that will help you recall your passwords."

After completing the second pass, participants were instructed to destroy their lists in a provided strip-cut paper shredder.

[1]Websites were collected from the researchers' web surfing histories. Additionally, the sites were collected from results of searching "login", "password", and "username" in Google.

4.2 Results and Discussion

Table 1 reports summary statistics for both the first and second passes of the study.[2] The number of accounts in the first pass is the number of successful login attempts, a conservative measure of the number of online accounts. The reported statistics from the second pass incorporate the information from the first pass; it was not an independent measure. There were fewer participants in the first pass than in the second pass due to noise introduced by requesting self-reported statistics. One participant was confused between the goals of the first and second passes; his observations were inconsistent and, therefore, dropped. One participant entered nonsense values for the first pass and these observations were dropped. We also altered two observations of password list length in the first pass as these observations were clear typos (e.g., a list length of "41" was reduced to "4" after discovering the number of successful logins was "4").

Out of the 139 sites presented to participants, they used a small portion of the sites ($N = 49$, $M = 6.67$, $SD = 3.34$. $Mdn = 6$). In the subset of sites where participants had accounts, they were largely successful at logging into these sites ($N = 49$, $M = 4.67$, $SD = 2.49$, $Mdn = 4$) and their password list length reflects this. Respondents indicated the first pass of the login task generally captured most sites participants used, where 24 of 49 participants said the first pass captured 75–100% of their websites and 11 said it captured 50–74% of their websites.

Password lists could include reused passwords—multiple entries of the same password. Actually, participants reported having only a few unique passwords, where half of the sample had three or fewer families in their list. Participants also tended to reuse a password without transformation rather than permuting a base phrase (e.g., appending a number of the end of a password). Using passwords in a theme was relatively unpopular, as the median use of related passwords was zero.

Participants averaged 2.43 failed logins ($N = 49$, $SD = 1.86$). This included timeouts ($M = .69$, $SD = .82$) where participants were unable to log into a website within 90 seconds. Table 2 lists the reasons why participants said they were unable to login to websites. Even though participants were asked to bring anything that would help them remember their passwords, they still had trouble recalling their usernames (46 times) and passwords (42 times). While participants had trouble recalling both usernames and passwords, the majority of failures were from forgetting either the username or the password rather than both (17 times). Unsuccessful logins were often for online shopping websites

[2]We considered the possibility that users had passwords that they reused with some transformation, such as appending punctuation or numeric characters. We defined several possible transformations and had users group these classes of similar passwords into "families." Thus, the reported statistic on the number of families is equivalent to reporting the number of unique passwords

	First Pass						Second Pass					
Variable	*N*	*M*	*SD*	*Mdn*	Min	Max	*N*	*M*	*SD*	*Mdn*	Min	Max
Number of Accounts	49	4.67	2.49	4	1	11	49	7.86	4.96	6	1	24
List Length	48	4.06	1.99	4	0	9	49	5.98	3.27	5	1	18
Number of Families	48	2.25	0.98	2	0	4	49	3.31	1.76	3	1	10
Size of Largest Family	46	2.87	2.01	2	0	8	49	3.35	2.35	3	1	10
Size of Smallest Family	47	1.43	0.93	1	0	4	49	1.33	0.94	1	0	5
Number of Repeated Passwords	48	3.06	2.19	3	0	11	49	3.76	3.96	3	0	25
Number of Related Passwords	48	0.77	1.34	0	0	7	49	1.18	1.62	0	0	5

Table 1: Descriptive Statistics for Activity Covered by Login Task

Reason	Frequency
Didn't know the account password	46
Didn't know the account username	42
Discovered didn't have an account	15
Needed multiple attempts	6
Didn't know the account number	6
Needed the registered e-mail address	4
Entered with typographical error	3
Couldn't access browser stored password	2
Other	6

Table 2: Reasons Cited for Failed Logins. Multiple responses allowed.

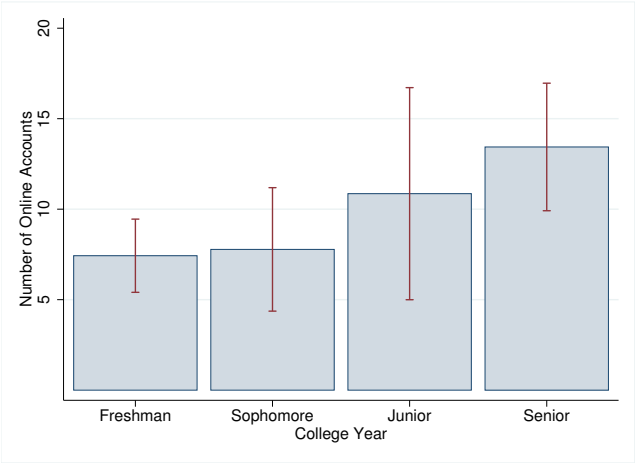

Figure 1: Mean number of website accounts by year of school with standard error bars.

(JCrew, Old Navy, etc.); students thought they had accounts but only used the sites for purchasing without logging in.

After using the initial suggestion of sites, participants reported other sites they used.[3] Although they were instructed to recall as many passwords as possible, participants still had few unique passwords ($N = 49$, $M = 3.31$, $SD = 1.76$, $Mdn = 3$).

If we quantify reuse as the number of online accounts per unique password, the median reuse rate differed slightly between the first ($N = 45$, $M = 2.18$, $SD = 1.12$, $Mdn = 2.33$) and second passes ($N = 49$, $M = 3.18$, $SD = 2.71$, $Mdn = 2$), although the dispersion (variance) between the two passes more than doubled. This due to the increased range of reuse rates. In the first pass, the reuse rates ranged from 0 to 5 while, in the second pass, reuse rates ranged from .25 to 14. We were unable to detect a difference between the reuse rates of those who used aids (laptops or paper notes) and those who relied on only memory in the first pass, $F(1, 44) = 0.71$, $p > .05$ as the effect size was small $\eta^2 = .01$; the small effect and the small number of observations led to a low power, power = .12. Similarly, no difference was detected in the second pass, $F(1, 48) = .04$, $p > .05$, $\eta^2 = .00$, power = .05. Participants received no significant benefit from using their own machines or their own browsers and even paper aids did not help significantly.

Although participants had relatively few accounts, they still reused their passwords. In fact, we expect that password reuse will become a bigger problem over time. Figure 1 shows that the number of accounts increased by year in school. This difference is significant[4] at an alpha of .05, $F(3, 42) = 3.81$, $p = .02$, $\eta^2 = .04$; people accumulate more online accounts as they get older. Yet, the number of unique passwords did not change by year of study, $F(3, 42) < 1$. People have more accounts over time, but they do not have significantly more passwords. Furthermore, reuse rates were positively correlated with the number of accounts in both the first pass ($r = .68$, $N = 45$) and the second ($r = 0.53$, $N = 49$). A scatter plot of the reuse rate and the number of websites for the second pass is shown in Figure 2. This plot demonstrates that people will reuse passwords more often when they have more accounts. These predict an increasing problem with password reuse: people will accumulate more online accounts as time passes, people will not generate significantly more passwords over time, and people tend

[3]Some participants reported categories of websites (e.g., "blogs") rather than actual site names. In this case, we underestimate the number of sites by counting each category as one site. Some participants also report internal university sites which use the same authentication ($N = 49$, $M = .55$, $SD = 1.00$, $Mdn = 0$). These internal site entries are ignored as they were captured in the original first pass list and would over-inflate the reuse rate estimates.

[4]One caveat is that the students were unevenly distributed by year with 17 freshman, 12 sophomores, 7 juniors, and 18 seniors.

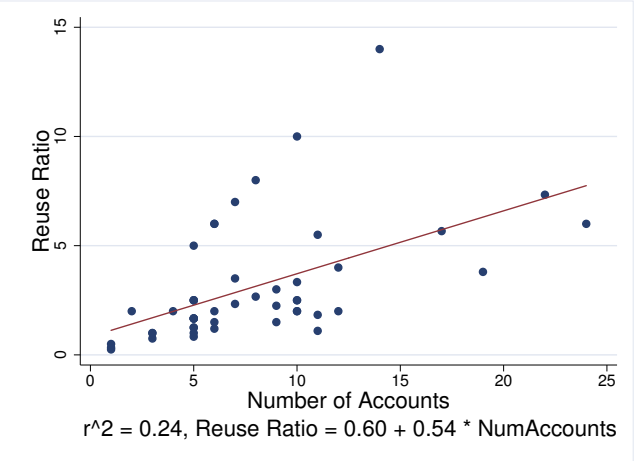

Figure 2: Plot of reuse ratio and the number of online accounts with login authentication in the second pass

to reuse passwords more as they have more accounts.

5. USER PRIORITIES

Our survey quantified what users were currently doing and we expect password reuse will be a bigger problem as people accumulate more online accounts over time. Yet, we need to also look at why people are reusing their passwords. Prior work has indicated that security is not a priority for users and that password authentication is seen as a nuisance rather than a protection [1]. We wanted to understand users' practices and their justifications for those practices.

Websites accounts are unusual in that many use password authentication in a fundamentally different way. The premise of password authentication is identifying the user to protect access to a resource. The motivation for the protection can have obvious benefit to the user, such as a PIN that prevents others from stealing funds. The motivation for protection may also be indirect, such as door codes that prevent outsiders from stealing from an organization. This protection is intuitively beneficial and this may obviously transferred to the online realm for websites that store financial data. For example, online banking systems, such as eZCardInfo.com, store VISA credit account information but also support money transfers from other banking accounts. Shopping sites also store financial information. Amazon.com stores credit card information and bank account information for its 1-Click shopping feature.

On the other hand, many websites are simply identifying users. Online newspapers, such as the online version of The Washington Post, use logins to track users rather than protect users' accounts. Another example is Wikipedia, which uses password authentication to identify users in histories of article changes. The identified users receive little benefit, as the mechanism is primarily for discouraging inconsiderate modification of articles. Outside of paid subscription services such as the online version of the Wall Street Journal, users receive no benefit from being identified. These systems burden the users with an additional password to manage. In addition, the accounts may remain available even when the user stops logging in. The user may forget these accounts exist, but the password state (the username and password) remain. Coupled with the likelihood that people reuse usernames and passwords, users are vulnerable to attacks where someone collects login information on one site and uses it to compromise an account on another site. In fact, Schneier suggests that creating a Trojan site will likely help an attacker compromise multiple accounts. First, the attacker may collect login information and guess other sites which have accounts with similar information. Secondly, the website could reject all login attempts. Since users can confuse their passwords, they are likely to enumerate through their limited set of passwords [22]. Thus, the attacker could compromise multiple accounts through a *single account's* login information but also could compromise multiple accounts through a *single user's* login information.

As alarming as these attacks may be, it is unclear whether these techniques are being employed by attackers. Identifying users without providing any incentive to protect password state is a problem as well though. Users are habituated to poor password practices with online accounts that merely identify users rather than authenticate them for their own protection. These sites encourage users to subvert the system. They may share registration information [5]. They may also follow poor password practices through either weak password selection or through password reuse. Essentially, these websites take a protection mechanism and turn it into an inconvenience that accustoms users to bad password habits.

Given this context, it would unsurprising to find users justify password reuse; however, it would also be valuable to contrast these excuses with explanations of how and why users avoid these practices. We can understand the forces that enable poor security habits but also what motivates users to do better. This section describes our results in studying user's behavior and the role technology has played in increasing password security.

5.1 Method

Participants. To reiterate section 3, this part of the study is based on the questionnaire administered to students before performing the login task. There were 58 participants (18 male, 40 female) although one participant did not complete the questionnaire.

Procedure. Participants took a 115-question survey. Questions covered demographic information, explanations of password reuse and avoidance, explanations of password creation and storage, and descriptions of password management methods. Participants were presented with both open ended questions and also statements using a 5-point Likert scale (1 = Strongly Disagree, 2 = Slightly Disagree, 3 = Neither Agree Nor Disagree, 4 = Slightly Agree, 5 = Strongly Agree) for responses.

5.2 Justifications of Password Practices

We asked participants if there were "two websites where you use the same password" and, if so, "why do these websites have the same password." As Table 3 lists, the most common reason for reuse was that it makes a password easier to remember. One participant wrote, "I usually use the same password or a variation of it, because that way I know I will always remember it." In fact, when responding to our questionnaire, participants strongly agreed with the statement "if I reuse a password, it is easier for me to remember

Reason	Frequency
Easier to remember	35
Have Too Many Accounts	8
Same Category/Class of Websites	7
Unimportant website	4
Too Difficult Otherwise	3
Only Use One Password	2
Other	3

Table 3: Reasons Cited for Using the Same Password. Multiple responses allowed.

Reason	Frequency
Security	12
Site Has Certain Information	11
Site Restricts Password Format	10
Important Website	7
Particular Category of Site	4
Other	12

Table 4: Reasons Cited for Choosing a Different Password. Multiple responses allowed.

it" ($M = 4.70$, $SD = .79$, $Mdn = 5$).

Similarly participants indicated any other approach would be more difficult, requiring them to track many accounts. Only four participants justified reusing a password because they didn't care about the account, as one participant wrote, "[the sites are] message board sites where it is not a disaster if someone were to crack it. I doubt anyone would take too much time trying to figure out my message board password. The only benefit would be to pretend to be me and post." As the quote suggests and we also suspected, people may categorize sites, where sites in the same category would use the same password. This would allow users to weigh the relative benefits of reuse against the increased security of avoiding reuse. Although anecdotal evidence suggested people followed this idea by maintaining levels of security, it was not cited as a common reason for reusing a password in the free-form question. Additionally, responses only weakly agreed with the statement "I have different passwords for different security levels of websites. For example, I have a generic password for online newspapers but I have a special password for my online bank account" ($M = 3.52$, $SD = 1.55$, $Mdn = 4$).

The result was somewhat ambiguous. Some people may categorize a website as "unimportant" and reuse a password while others might turn to a service like BugMeNot.com; participants did not justify reuse in unimportant websites: "I reuse a password if it is unimportant to me" ($M = 3.21$, $SD = 1.56$, $Mdn = 3$). Rather than justifying reusing a password on unimportant websites, people may prioritize creating unique passwords for important sites. What information qualified as important?

Students placed a higher priority on avoiding password reuse when the website contained financial data or personal communication in comparison to health information. Students agreed that "I reuse a password when there isn't much financial information (bank account, credit card number, etc.) about me on a website" ($Mdn = 4$), that "I reuse a password when there isn't much personal information (sexual orientation, health status, etc.) about me on a website" ($Mdn = 4$), and that "I reuse a password when I use a website for routine communication (e-mail, chat, etc.)" ($Mdn = 4$). Wilcoxon's matched-pairs signed rank test[5] was significant when comparing responses to protecting financial information over health information ($T(57) = 3.25$) and when comparing protecting personal communication over health information ($T(57) = 2.30$). Responses to protecting financial information versus personal communication was not significantly different ($T(57) = .01$). This sample was particularly concerned with protecting their correspondence and their financial information but was less concerned about their health information. We suspect this is because students are young and their health status generally does not affect their careers or insurance.

Protecting private information may motivate people to create unique passwords. We asked participants if there were "two websites where you use different passwords" and, if so, "why do these websites have different passwords." Table 4 shows that, for responses to this open-ended question, one of most cited reasons was security; many were particularly concerned that having the password to one account would help an attacker compromise another account: "I don't like to think that if someone has one of my passwords, she or he could access all of my information for all pages I log into." Another common reason was protecting information, such as financial data: "I don't use my 'less secure' password for accounts that contain credit card information, etc." Similarly, people explained that some websites were more important than others, "for less important accounts, I use an easy password for simplicity."

An important factor in creating a unique password was restricting the format. These websites effectively prevented reusing an old one. As one participant wrote, "different websites have different system requirements for passwords, such as some require a certain amount of capital letters, or numbers, or password length, etc." Participants generally agreed that they have had experience with this problem: "I wasn't allowed to use one of my passwords because it wasn't in the correct format (too long, too short, did or didn't have numbers, did or didn't have punctuation, did or didn't use capitals, etc.)" ($M = 3.83$, $SD = 1.37$, $Mdn = 4$).

The reasons for avoiding password reuse in Table 4 highlight the situations where users might be amenable to using technology to help them manage passwords. They avoided reusing a password when then believed they needed increased security. They agreed that "it is harder to guess my password if I use different passwords on different websites" ($M = 3.70$, $SD = 1.19$, $Mdn = 4$) and that "it is harder to gather information about me if I use different passwords on different websites" ($M = 3.75$, $SD = 1.08$, $Mdn = 4$). This leads to a pragmatic problem, however. While increased security is warranted for important websites, participants also agreed that "it is unrealistic for me to periodically create

[5]When comparing responses to two questions, we test differences in medians using Wilcoxon's Matched Pairs Signed Rank Test (T). While the t-test would be appropriate for interval measures, Likert responses were not always normally distributed, so we chose the nonparametric version of the t-test.

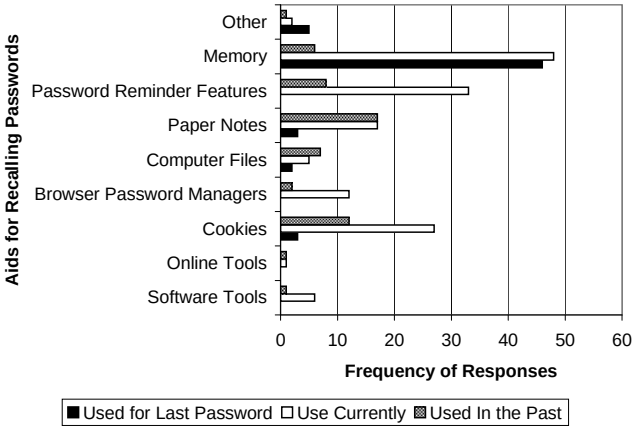

Figure 3: Aids Participants Cited Using to Help Recall Passwords. Multiple responses allowed.

new passwords" ($M = 3.78$, $SD = 1.15$, $Mdn = 4$). They would like to avoid password reuse in some circumstances, but it is difficult to do so. One solution is automatically generate a password for new users; however, participants strongly disagreed that "if a password is generated for me by a website than I use this password instead of one of my normal passwords" ($M = 1.69$, $SD = 1.23$, $Mdn = 1$).

There could be several reasons why participants do not use passwords that are generated for them. First, these passwords are often temporary and users are given specific instructions to immediately change the password to something different than what was generated. Secondly, people may want to reuse their password—they could just change the generated password into something they commonly use for an unimportant website.

5.3 Methods of Storing Passwords

Although participants avoided generated passwords, we wondered what kinds of tools participants were comfortable using. We surveyed the participants to determine what they used to help manage their passwords. Participants were instructed to think about the last time they created a password and were asked where they stored their last password. As shown in Figure 3, participants relied on their memory. We also asked participants to select which aids they used currently to manage their passwords and which aids they had "used in the past but no longer use." Again, memory was more commonly used than any computing technology, but the technology only partially helped. Participants also relied on password reminders such as a website feature that asked "forgot your password." This mechanism often relies on e-mail authentication to, in turn, authenticate the user. An e-mail is sent to the user's registered address, which either sends the password or provides the means for resetting the password. On the one hand, this method is convenient when users need to access websites but, on the other hand, this method relies on recalling the registration information and having access to a predefined e-mail account. This method is also inconsistent across websites and users may experience a delay between when they want to access an account and when they can finally do it.

Participants also indicated they relied on website cookies, given the example of "Website checkbox: 'Remember my password on this computer.'" Like using password reminders, when people use cookies, they are not recalling their password at all. There are disadvantages to using cookies. Users must avoid logging in from another machine (which requires recalling the original password); they must avoid clearing their cookie cache; and they must expect no other user will log in to the same website on the same machine with another account.

Using cookies may also make users more vulnerable. While the New York Times's online newspaper users authentication to track users, traditionally, password authentication protects access. If users are accustomed to using cookies, they may inadvertently expose financial data. For example, when someone uses cookies in Amazon.com, they implicitly agree to purchases whenever someone accesses the same browser.

While paper notes such as Post-it notes, a notebook, or a day planner were the most commonly abandoned tool, the digital equivalents were relatively unpopular. Few users claimed to use an online password manager like Gator eWallet or PasswordSafe.com, and few claimed to use software password managers like Password Agent, Password Tracker, or Any Password. Instead, they used managers embedded in their browsers such as Internet Explorer's AutoComplete, Netscape's Password Manager, and Firefox's Saved Passwords. Even this was relatively unpopular. These features were less popular than relying on memory. Yet, when users rely on their memory, they have to store, recall, and type their password rather than having it automatically collected and filled in. Some people may be concerned that these features are vulnerable to attack. Like cookies, browser password managers could allow unintended users access accounts they should not.

Browsers password managers also tie users to a particular browser on a particular machine. The issue may be obsolete if applications like Portable Firefox became more popular. Portable Firefox is a zipped version of the Firefox browser that can be stored on portable devices such as USB jump drives. Portable software would provide the benefits of browser password managers without the problems mentioned earlier.

6. USER MODELS OF ATTACK

In this section, we discuss users' perceived threat models for what they believed made a strong password and for who they believed was likely to attack their online accounts. This work is pertinent to understanding the adoption of aids for managing passwords as the results offer insight into who participants believed their passwords needed protection from and how they understood password strength.

6.1 Perceived Threat by Others

We first consider who participants saw as likely attackers to online accounts. We wanted people to consider situations where someone would feel motivated to attack and also to gauge their ability to attack online accounts. We were interested in seeing if motivation or ability had a greater weight in perceiving someone as likely to attack an online account.

6.1.1 Method

Participants. Participants completed the attacker ranking section of the study in conjunction with the password management questionnaire in the first session (57 observations).

Procedure. Participants were first provided with examples where a password could be compromised. For example, "a stalker could guess a password after learning some personal facts, like a pet's name or a social security number." The online questionnaire then asked participants to rank types of people by their likelihood to compromise passwords. While we would have preferred to present categories with all combinations of three independent characteristics (personal relationship, computer expertise, affiliation), we believed this would have been too many choices for meaningful rankings. Instead, the population was partitioned unevenly: someone you know well (abbreviated as "friend" in this paper), someone without computer expertise that you have met ("acquaintance-nontech"), someone with computer expertise that you have met ("acquaintance-expert"), someone from your organization that you do not know ("insider"), someone from a competing organization that you do not know ("competitor"), and someone that is unaffiliated that you do not know ("hackers").

The instructions first told participants, "ignoring their motivation, for each person listed below, write at least one scenario where this person could obtain one of your passwords." Afterwards, participants were asked to rank the six categories of attackers three times. In the first ranking, participants were asked to rank attackers by their ability to "access information without permission from one of your web accounts."[6] They were instructed to ignore motivation and consider ability only. In the second ranking, participants were instructed to rank people by their motivation to compromise passwords, "ignoring ability and considering motivation only." Finally, participants were asked to rank attackers by their likelihood to attack an online account, "considering motivation and ability."

6.1.2 Results and Discussion

While the rankings themselves might prove interesting, we focus on the extreme ends of the rankings, those considered most and least likely, able, or motivated to attack respondents' accounts.

Considering the ability ranking, users' perceived threat models might emphasize attacks from hackers, but our findings suggest that users realized the threat posed by those closest to them. Friends were considered most able attackers (51.79% of 56 responses). Surprisingly, only 10.71% of respondents thought a hacker who had no personal connection would be the most able attacker. In fact, 35.19% (19 of 54 respondents) said an "unaffiliated stranger" would be *least* able to compromise their passwords.

In the motivation ranking, most respondents (62.50%) indicated that a competitor or a hacker was the most motivated to attack and that a friend or an acquaintance without technical experience would be the least motivated. This is the typical response we would expect, as one respondent explained:

> Anyone who wants to [compromise a password] can, you don't need to know them, and the shield of anonymity may make it less morally reprehensible to do so.

This is even considered a normal belief of who would attack:

> This is my standard perception of identity theft, where retaliation from young people or hackers tops the list.

Yet, a minority of participants had an opposite ranking. Overall, a quarter of responses (15 of 56) noted that a friend would be *more* motivated than a hacker. A quarter of responses said a hacker would be *least* motivated. In fact, 9 respondents (16.07%) said that a friend would be most motivated and a hacker would be least motivated. We were surprised by this result, as we believed people assumed those who had a personal relationship would be most trustworthy. A few respondents mentioned those closest to them had more opportunities to build ill will:

> My ex-boyfriend falls into the top category and I'm concerned....

Two female participants, including the above participant, revealed that former boyfriends had or possibly had attacked their accounts. This is consistent with work by Dourish et al. which observed female office employees were concerned about stalking [8]. Other participants mentioned that a personal tie made a familiar attacker motivated by curiosity:

> The closer they are, the more curious they may be.

When considering overall likelihood of compromise, participants seemed to weigh both motivation and ability. We used a fixed effects logistic regression of all six types of people to predict the odds of considering an attacker most likely to compromise a password based on 1) their ability and 2) on their motivation. This enabled us to separate the effects (and thus assess the relative importance) of perceived ability and perceived motivation on ranking someone as likely to compromise a password. When an attacker is perceived as very motivated, the odds of considering him/her a likely attacker are multiplied by 6.28 (or $e^{1.34}$), regardless of the type of person (friend, hacker, etc.) or their ability. When people perceive someone as having great ability to compromise their password, the odds of considering him a likely attacker are multiplied by 3.82 (or $e^{1.83}$), regardless of the type of person or their motivation. Both effects are significant at the .05 level. The effects of ability and motivation on perceived likelihood to attack are strong, and the effect of motivation is stronger than the effect of ability on perceived likelihood of attack.

The responses to the motivation and likelihood rankings indicated that respondents subdivided into two camps, the first believing those closest to them would be interested and would likely attack their online accounts while the remaining thought that hackers were the most motivated and likely attackers. Motivation has a strong effect on perceived likelihood of attack. One possible explanation is that gender affected the rankings, as women might be more concerned about stalking; however, the distribution of the most motivated attacker rankings was independent of gender.

[6]Although we describe the categories of people as "attackers" in this paper, we avoided using "attack" to describe compromising passwords as we predicted people would only consider those with malicious intent. By saying the passwords were compromised "without consent," we ignored the situations where someone would willingly disclose their password.

Participants believed those closest to them had the greatest ability to compromise their passwords. This is consistent with Petrie's hypothesis that passwords are one word personal identifiers: those closest to the respondents are most able to guess the content [16]. Notice that hackers are considered *least* able to compromise passwords—it was as if users believed using personal identifiers was safer because cracking the passwords required personal knowledge rather than expecting these are common identifiers available in dictionaries.

6.2 Perceived Strength of Passwords

If users expect that having a personal connection to the attacker presents an advantage, we also expect that this influences what users perceive as strong passwords. We were interested in seeing what users thought were strong passwords. For example, our school provides a webpage that explains how to create strong passwords [18]. We wondered if students understood these tips.

6.2.1 Method

Participants. Participants completed this part of the survey in conjunction with the login task in the second session (49 participants).

Procedure. Participants were presented with the following scenario:

> Many websites have tips and rules for creating strong passwords. Pretend your friend Eve Jones (evjones@princeton.edu) is also a student at Princeton and she is having trouble understanding these rules. For each rule or tip, she's provided three example passwords with an explanation of how she created her password. Help her learn what makes a strong password by ranking her examples from strongest to weakest and explaining your ranking.

This was followed by a series of eleven statements which were chosen by finding webpages that suggested methods for creating stronger passwords:

1. Use uppercase and lowercase letters in the password.
2. Use a password of at least six characters.
3. Avoid common literary names.
4. Mix up two or more separate words.
5. Create an acronym from an uncommon phrase.
6. Avoid passwords that contain your login ID.
7. Use numbers in the password.
8. Avoid abbreviations of common phrases or acronyms.
9. Drop letters from a familiar phrase.
10. Use homonyms or deliberate misspellings.
11. Use punctuation in the password.

For each participant, statements were presented in a random order. Additionally, the three example passwords were presented in a random order. We tried to construct the passwords so they were approximately equal in length except for the case where increasing length was a suggestion. As we needed to create short explanations, all of the passwords were relatively weak. Each included some randomness, whether it was a randomly capitalized letter, a randomly selected set of characters, or a randomly added or subtracted character. In our explanations, we avoided the use of the word "random" which would likely influence the rankings. One example password was "01/12/85" and it's explanation was "this is my birthday." An example of a random password was "snyfe", which had the explanation "I took the first or last letter of words at the end of paragraphs in an excerpt from the Undergraduate Announcement: (s = interests, n = information, y = year, f = field, e = education)."

6.2.2 Results and Discussion

We collected responses to the rankings and a cursory analysis indicated that participants understood that randomness was beneficial to password strength, but they linked this to human guessability. If this was the case, the explanations of password rankings would frequently describe human attackers and include some notion of randomness. With a total of 17,035 words collected from participants' password rankings, we constructed a word frequency list and checked if these terms occurred regularly. Removing parts of speech such as articles and conjunctions from the list, the following words are top ten unique words and their frequency of occurrence: it (408), one (252), password (221), secure (217), random (215), most (180), guess (176), letters (172), not (169), first (157).

Password strength was indicated by the words "secure" (217), "random" (215 and "randomly" - 11 and "arbitrary" - 11), "common" (89 and "commonly" - 14 and "obvious" - 39), "crack" (13), and dictionary (10). Having common words or phrases was seen as a negative quality (for example, "the third is least secure because it's a common word backwards") while having randomness was seen as a good quality (for example, "the password incorporating personal information is the least secure, whereas the first two are more random"). Although participants did not use security terminology, the prevalence of randomness and commonness in their explanations implies users understood they could avoid terms that are frequently used in passwords. Yet, respondents rarely mentioned cracking using dictionaries. In fact, "hack" only occurs 7 times, with "hacker" (1) and "hack" (1) also appearing infrequently.

We believe that participants conceptualized attacks from a human using a guess-and-check technique. They frequently referred to "guess" (176) and related words: guessed (26), guessable (11), guessing (4) deduce(d) (4). Participants would write things such as "[the] 1st because its fairly simple to learn but not a word someone would guess." Guessing was often equated with a human attacker guessing the password. Participants frequently referred to people: "someone" (69), "people" (56), "anyone" (27). For example, participants would write "the last one is very obvious to anyone who knows the user" or "The first one though is just nonsense and random so I doubt anyone could guess it." Participants also discussed accumulation of knowledge: "know"

(39), "knows" (36), "known" (17), and "knew" (10). In particular, people indicated that knowing the victim would help crack a password: "PrincetonNJ is too easy for someone to guess if they know where you live" or "one would have to know her decently well to know her favorite novel." These explanations overlook the common techniques for cracking passwords. Humans may guess how a password is constructed, but they can use automated tools for enumerating all of the possible choices. They can do this without directly knowing personal information. Dictionaries can store combinations of all cities and states, all valid telephone numbers and social security numbers, and many phrases from literature. Yet, participants associated this content with personal knowledge. Preferably, users would understand that people have common techniques for creating passwords and these passwords could be cracked given enough attack attempts and provided with large enough potential password lists.

7. SURVEY IMPLICATIONS

How can we practically encourage users to avoid reusing passwords? They see creating new passwords as difficult and they see avoiding reuse as helping increase security, yet they see using more than a few passwords as onerous strain on their memory. Technological solutions could help in each of these cases. There are several tools for generating passwords and tools for generating passwords in specified formats. People can avoid reuse when a computer stores and retrieves a password (or in the case of stateless password managers, regenerates a password). This lightens the memory burden.

Despite the evidence that users rely on their memory, few technological solutions support that habit. Instead of helping users recall their passwords, many tools hide passwords from users. The incentive to use a browser password manager is that it keeps users from retyping their password when logging into a website. At the same time, this also prevents the user from learning their password and increases their dependence on a particular browser. Assuming people are not using portable browsers, this convenience becomes an annoyance when they need to login from another location. Instead of just storing the passwords and filling in forms for the users, the browser could help users learn their passwords. For example, rather than filling in the password, the browser could display it with a low-contrast background. This could help remind users what their passwords are—it matches a website to specific login information. Once the association is learned, the user could stop using the browser feature and rely on their memory. Thus, users could be helped to create strong, unique passwords through generators and remember the passwords with browser hints.

Websites could also change the way they authenticate users. Any site that sends password reminders over e-mail essentially uses e-mail to authenticate the user. It inherently expects users receive e-mail messages quickly. Websites could provide another mechanism for authenticating users, however. Instead of querying usernames when users forget their passwords, websites could ask users to provide an e-mail address, check their registration data for a match, and send an e-mail to that address. From the message, users could be directed to a page that not only logs them in, but also installs a cookie that identifies the user. Each time the user logs in from a different machine, they could repeat the process. The benefit of this system is that it relies on a single password that the user places on a single server rather than allowing the user to distribute this information across multiple websites or to use a single service (such as Microsoft Passport) that distributes this information across multiple websites. This approach would not weaken the security of systems that already use e-mail for password recovery or reset. Anyone who had access to the victim's e-mail account could already compromise these existing systems. This removes password state and also eliminates a situation that promotes password reuse, but business incentive structures may not support alternative authentication systems.

We could also promote better password security practices. When registering at a new website, users select a unique password. Once chosen, there is little incentive to change a password—in fact, participants agreed that "I don't have a reason to change the password on the websites I use" ($M = 3.58$, $SD = 1.26$, $Mdn = 4$). Unfortunately, when a user creates an account they have little motivation to generate a unique password. They have not started storing private or financial information on the website. Reuse is encouraged because it makes a password easier to remember. Furthermore, with a new account, the site is not important yet and users cannot predict how often or frequently they would use the account in the future. Even with online stores, users may not store financial information until they become accustomed to shopping at the store. In sum, when they register with a website, they have not yet disclosed anything worthy of protecting with a password.

As time passes and after building a relationship with a website, users are locked into their reused password. Once they have started reusing a password across multiple sites, not only would it be a burden to remember a unique password, they would have to remember which site had the new password. Participants agreed that "I try to use the same password for multiple websites, so it would be inconvenient to change the password" ($M = 3.84$, $SD = 1.25$, $Mdn = 4$). Compounding the problem, websites rarely ask participants to change their passwords. Websites need to attract and retain users; enforcing security policies might drive users away.

If sites avoided authentication before users invested private information, the websites could transition users to password authentication. The sites could choose a time when users are motivated to protect an account and when users understand the benefits of avoiding password reuse. Again, the vendors may have little incentive to do this, but we can also push the solution to browsers.

While browser password managers ask users for permission to store newly entered login information, they do not monitor online use of website accounts. Browsers could notice frequent use of an account and suggest refreshing that account's password. In fact, our participants strongly agreed that "I will change a password if I have been asked to change it" ($M = 4.25$, $SD = 1.00$, $Mdn = 5$). Currently, browser password managers and stateless password managers interrupt the user's behavior when they have the least motivation. Instead of presenting a stronger password or suggesting easier password management at an appropriate time, the browsers present their benefits when the user is unaware of the problem. Instead, the browser could use browser history as a sign of trust development, as suggested by Yee [27]. Once the user has returned to a site multiple times, the browser could suggest that changing the password to something stronger because it appears the site has grown in

importance.

8. CONCLUSIONS

While multiple papers have studied password security, our work has developed a broad description of password management strategies for online accounts. Like other papers, we quantified password reuse, but our unique method allowed us to measure results with actual login attempts rather than relying on participants to recall website use. Our method also elicited explanations for why participants had trouble with logging into websites and demonstrated that using memory aids or a personal laptop had a negligible benefit for password management. The questionnaire on password management strategies also demonstrated that people relied on their memory. Even though people have access to a computer and the Internet when logging into online accounts, we were able to show the technology they used did not help them with recalling their passwords. Current tips for strengthening passwords also fail to explain the nature of dictionary attacks. While participants understood the benefit of having randomly generated passwords, they still pictured human attackers and strengthened passwords by making it difficult for a human to guess them. This was demonstrated when participants ranked those closest to them as having the greatest ability to compromise their accounts. Participants suggested that simply knowing personal information would be beneficial to compromising a password. This implies users understood personal information might be used in the construction of a password and that some words or phrases may be commonly incorporated; however, the model fails to account for the construction of dictionaries which could enumerate these possible passwords without having a personal connection to the victim.

Our findings also indicated that the nature of online accounts and tools for managing passwords in online accounts enable poor password practices rather than discourage them. There is a gap between how technology could help and what it currently provides. Our study was specifically interested in how technology could be used to ameliorate the problem of password reuse and our participants came from a technologically savvy demographic: they are both well-educated and well-connected. According to Princeton University's Student Computing Initiative, 90% of last year's incoming freshman owned their own computers and used the campus network service. Over half of our participants used their own laptops when they came into the lab. We could argue that the students represent the forefront of what to expect with online activity: these users easily adopt new technology and have a culture of computing. Yet, our findings indicated that despite their technical abilities and education, they still had trouble understanding the nature of some attacks. Rather than hinting at impending proliferation and adoption of new password management tools, these students demonstrated that the available technology has not aided password management. Furthermore, they demonstrated that password reuse is likely to become more problematic over time as people accumulate more accounts and having more accounts implies more password reuse.

9. ACKNOWLEDGMENTS

This material is based upon work supported under a National Science Foundation Graduate Research Fellowship. Any opinions, findings, conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the National Science Foundation.

10. REFERENCES

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

[2] R. J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, Inc., New York, NY, USA, 2001.

[3] S. Brostoff and M. A. Sasse. Are passfaces more usable than passwords: A field trial investigation. *People and Computers XIV - Usability or Else: Proceedings of HCI 2000*, pages 405–424, 2000.

[4] A. S. Brown, E. Bracken, S. Zoccoli, and K. Douglas. Generating and remembering passwords. *Applied Cognitive Psychology*, 18(6):641–651, 2004.

[5] BugMeNot.com. Frequently asked questions. `http://bugmenot.com/faq.php`. Accessed 5 March 2006.

[6] J. Bunnell, J. Podd, R. Henderson, R. Napier, and J. Kennedy-Moffat. Cognitive, associative and conventional passwords: Recall and guessing rates. *Computers and Security*, 16(7):641–657, 1997.

[7] R. Dhamija and A. Perrig. Dejà vu: A user study using images for authentication. In *Proc. of the 9th USENIX Security Symposium*, 2000.

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

[9] E. Gabber, P. B. Gibbons, Y. Matias, , and A. J. Mayer. How to make personalized web browsing simple, secure, and anonymous. *Financial Cryptography*, page 1732, 1997.

[10] J. Goldberg, J. Hagman, and V. Sazawal. Doodling our way to better authentication. In *Proc. of Ext. Abstracts CHI 2002*, pages 868–869, New York, NY, USA, 2002. ACM Press.

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

[12] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin. The design and analysis of graphical passwords. In *13th USENIX Security Symposium*, pages 1–14, 2004.

[13] A. H. Karp. Site-specific passwords. Technical report, Hewlett-Packard Laboratories. `http://www.hpl.hp.com/personal/Alan_Karp/site_password/site_password_files/site_password.pdf`.

[14] D. V. Klein. "Foiling the cracker" – A survey of, and improvements to, password security. In *Proc. of the second USENIX Workshop on Security*, pages 5–14, Summer 1990.

[15] R. Morris and K. Thompson. Password security: a case history. *Commun. ACM*, 22(11):594–597, 1979.

[16] H. Petrie. Password clues. `http://www.centralnic.com/news/research`. Accessed 2 May 2005.

[17] J. Preece, Y. Rogers, and H. Sharp. *Interaction*

Design: Beyond human-computer interaction. John Wiley And Sons Inc., 2002.

[18] Princeton Office of Information Technology. Tips for creating strong, easy to remember passwords. Accessed 6 March 2006.

[19] S. Riley. Password security: What users know and what they actually do. `http://psychology.wichita.edu/surl/usabilitynews/81/Passwords.htm`, February 2006.

[20] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. C. Mitchell. Stronger password authentication using browser extensions. *14th Usenix Security Symposium*, page 1732, 2005.

[21] 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.

[22] B. Schneier. *Secrets and Lies : Digital Security in a Networked World*. Wiley Computer Publishing, New York, NY, 2004.

[23] D. Weirich and M. A. Sasse. Persuasive password security. In *Proc. of Ext. Abstracts CHI 2001*, pages 139–140, New York, NY, USA, 2001. ACM Press.

[24] D. Weirich and M. A. Sasse. Pretty good persuasion: a first step towards effective password security in the real world. In *Proc. of NSPW 2001*, pages 137–143, New York, NY, USA, 2001. ACM Press.

[25] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon. Authentication using graphical passwords: effects of tolerance and image choice. In *SOUPS '05: Proceedings of the 2005 symposium on Usable privacy and security*, pages 1–12, New York, NY, USA, 2005. ACM Press.

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

[27] K.-P. Yee. How to manage passwords and prevent phishing. `http://usablesecurity.com/2006/02/08/how-to-prevent-phishing/`, February 2006. Accessed 5 March 2006.