Passwords: Do User Preferences and Website Protocols Differ From Theory?

Roberta Ann Barra, University of Hawai'i at Hilo - Hilo HI USA
Roberta.barra@hawaii.edu

Alexander McLeod, University of Nevada - Reno, Nevada USA
amcleod@unr.edu

Arline Savage, California Polytechnic State University - San Luis Obispo CA USA
savage@calpoly.edu

Mark G. Simkin, University of Nevada - Reno, Nevada USA
simkin@unr.edu

ABSTRACT

Despite the availability of superior authentication tools, password security continues to be an important access control in modern, computer-based systems. Are strong passwords used in these systems? Under what conditions are users willing to adopt stronger passwords? To answer these questions, the authors examined the websites of 154 organizations and additionally, analyzed 240 responses from a separate survey of password users. In terms of password length and duration, the answer to our first question was "No, strong passwords are not used." The answer to our second question regarding willingness to adopt stronger passwords appears to depend upon how often users must change them.

KEY WORDS

Authentication, Access Security, End-User Controls, Password Protocols, Strong Passwords

INTRODUCTION

Although most security experts believe that "password authentication" is one of the weakest forms of personal identification, password security continues to be the verification procedure of choice for the vast majority of commercial and financial authentication systems on the web (Kubota, 2008). In fact, it is difficult to overstate the importance of password security, given the global use of alpha-numeric and graphical passwords for authentication (Ozok & Holden, 2008).

Passwords serve several functions. One is as personal identifiers—enabling computer systems to separate bona fide users from hackers. Another is as security gatekeepers—for example, enabling web developers to protect customer accounts from disruptive or harmful modifications. Finally, password security is an important part of corporate internal control. This is because passwords often control access to an organization's most important asset—its corporate data. This function is so important that the Information Systems Audit and Control Association's (ISACA) *IS Standards, Guidelines and Procedures for Auditing and Control Professionals* mentions "passwords" over 35 times (ISACA, 2007), and makes clear that password security is an integral part of an organization's internal control framework.

In this paper, the term "password protocol" refers to the policies governing the creation, persistence, and use of a password in a given application. Barra and Griggs (2007) show that, in the area of security, controls are often first developed by "common sense" and then refuted by rigorous research done mostly by scholars. Consistent with this paradox, the "common sense" approach to developing password protocol suggests that users be permitted to create shorter passwords that are changed frequently, while research indicates that minimum password lengths should be much longer and do not need to be changed until there is a known breach.

Because users often manage as many as 15 separate passwords (Florencio & Herley, 2007), the desirability of using strong passwords contrasts with the convenience of using the same, simple, short, easily-remembered ones repeatedly (Ives, Walsh, & Schneider, 2004; Webber, Guster, Safonoy, & Schmidt, 2008). The empirical evidence to date suggests that, unless forced to do otherwise, users (1) notoriously select easily-guessed passwords, including "password," "abc123," and "Jordan23," (2) actively resist changing them, and (3) often make little effort to protect them (Furnell, 2007; Howard, 2006; Wolfe, 2006).

How well does current practice reflect what we've learned about good passwords? For example, have the results of the academic research been implemented in practice? Are website password requirements and theory converging to form more secure systems? Are users willing to change their weak passwords? The next section of this paper reviews the relevant literature on this subject while the section after that describes a new study we conducted to answer these questions. The fourth section of our paper presents our results and also offers some caveats that limit the generality of our findings. The final section of the paper summarizes our study and provides our conclusions.

LITERATURE REVIEW

"Confidentiality" is an important part of web security. It relies on various authentication mechanisms to achieve these protective goals. To ensure confidentiality, for example, websites must identify users and verify that they are who

they say they are. This *authentication mechanism* typically requires organizations to develop policies concerning password length, composition, and duration, which then drives users to create or revise their online passwords (Gaw & Felten, 2006; Walsh, Ives, Louwers, & Schneider, 2006).

Authentication

There are many ways for websites to authenticate users—methods which differ in cost and convenience to both organizations and users. Historically, users have validated their identities by providing verification of, (1) *something they have*—for example, a token, smartcard or key, (2) *something they are*—for example, a biometric pattern such as a fingerprint, iris, retina, voice or behavioral pattern, or (3) *something they know*—for example, a secret such as a password (Cole, 2001). Verification mechanisms other than "secrets" often require an issuing authority and increase authentication costs (Florencio & Herley, 2007).

User Password Preferences

User preferences contrast sharply with security dictates regarding passwords. For example, a user's memory appears to be the limiting factor in password creation, affecting both the number of passwords that users can remember as well as their complexity (Dixon, 1987; Gaw & Felten, 2006). For these reasons, users generally restrict themselves to five or six passwords, which they use repeatedly in applications requiring them (Dixon, 1987; Florencio & Herley, 2007). Similarly, users often reduce the character sets from which they create their passwords—for example, to lower-case letters—thereby limiting the characters that hackers must guess and weakening the password itself (Grampp & Morris, 1984). Finally, some users simply choose to create the shortest password possible, even though weaker passwords translate into greater probabilities of compromise (DeAlvare, 1990).

Website Password Policies

Most websites place the burden of strong passwords on users, as illustrated by the recently discovered Gmail vulnerability (Harthun, 2009; ISecAuditors, 2009). Historically, the 1985 Department of Defense (DOD) definition of strong passwords was the industry standard (DOD, 1985). More recently, rigorous research has begun to replace the "common sense" approach developed by the DOD. But are websites now requiring users to create stronger passwords?

In an effort to address account security, Facebook added a one-time password feature (Prince, 2010). Problems with weak password security affect all sectors including government as detailed in Wired Magazine (Zetter, 2010) when an Internet voting system was hacked. Issues associated with passwords, such as stolen accounts, phishing, spam and viruses have reached a level where coping behaviors are detailed

in the press (Richmond, 2010). Weak passwords are said to be the enabler of malware and those who would do harm.

Security experts suggest that website password policies should be based on the risks associated with compromising the products or services provided (Kubota, 2008). Most administrators understand this premise and therefore assume that strong password policies will reduce the risks of an attack (Cole, 2001). But creating strong passwords requires users to (1) include more characters in their passwords, (2) expand the diversity of the character set used to create them by including capital letters, numbers and special characters, and (3) shorten the life of their passwords (FBI, 2002; NIST, 2006). Organizations pondering the options for what type of password authentication to use often choose alpha-numeric passwords for authentication purposes, shifting the burden for strong password creation to the user.

Given the continuing popularity of passwords for security purposes, it seems logical that companies and government organizations would require users to create strong passwords. Yet, what constitutes strong passwords is not clearly defined in the literature. Fordham and Furnell (2008; 2007) rely on the Department of Defense (D.O.D.) 1985 password protocol that establishes a "common sense" approach to establishing control protocols (Barra & Griggs, 2007). The D.O.D. protocol requires that passwords be difficult to guess and changed often. Mechanically, such passwords should have (1) a length of at least 10 characters, (2) a mixture of letters and numbers, (3) letters that are case sensitive, and (4) passwords with short life spans. Cole (2001) recommends password lengths of at least 10 characters.

With regard to short life spans for passwords, the theory is that shorter password durations limit the window of opportunity for password cracking or, if breached, for damage (Furnell, 2007). Other scholars theorize that the frequency with which users change their passwords should also depend upon the importance of the information guarded by the passwords themselves—for example, monthly or quarterly for relatively low-priority applications, but daily or even hourly for critical ones (Fordham, 2008).

Recently, scholars have begun to test the password protocols put forward by the D.O.D. and others with some surprising results. For example, Cazier and Medlin (2006) found that passwords with 10 or more characters could not be cracked with cracking software. Similarly, Wakefield (2004) found that it would take a computer 118 years to try those same combinations, thus making passwords with 10 or more characters virtually crack-proof. Finally, Howard (2006) concluded that changing passwords in the absence of a known breach was a waste of time and that passwords of 11 or more characters were superior for security against cracking.

A NEW STUDY

How well do online websites and end users apply what we have learned about password-protocol theory? This section of the paper describes two studies we conducted to answer this question.

Methodology and Research Questions

Our first study was an analysis of the password protocols used by various for-profit, non-profit, and governmental entities in online applications. The second was a survey of individuals now using passwords for internal security. In the first study, we examined website protocols with respect to the password length and composition, as well as any requirements for changing passwords. To do this, we searched the Internet using available search engines for the terms "password length", "password policy" and "how often to change passwords", and examined the first 300 URL results. An examination of the 300 results identified 154 websites that included password length and policy protocols.
Examining website password protocols allows us to see if there is any consensus concerning password protocols. If current password protocols continue to be based largely on "common sense" rather than on theory, then this should lead to a wide range of protocols rather than consensus because what seems like "common sense" to one person may not seem like "common sense" to another. Consequently, our first research question concerning password protocols was:

Q_1: Are website password protocols consistent as to required password length or duration?

The consensus on password lengths in the literature is that passwords should, *at a minimum*, be 10 or more characters in length. Howard (2006) suggests that "11 characters" is the minimum required length but adds that people are unwilling to use such long passwords. To test this supposition in our second study, we surveyed password users with the survey instrument shown in the Appendix to determine their password preferences and experience. Respondents included students, faculty, and business people from four separate universities, as well as several non-university settings.

Of particular interest to us were user preferences regarding password durations and lengths. We asked users what password length they would be willing to use if website protocols required them to change the password on a regular basis. We also ask respondents how long a password they would be willing to use if they did not have to change their password.

Survey questions about password lengths were asked in two different ways. First, we asked respondents whether they would be willing to use an 11-character password.

Then we asked whether they would be willing to add 3, 4, 5, 6 or more characters to their existing password. The addition of these characters would cause most people to create an 11-character password, but the second question frames the issue differently. We did this as an internal validity check for our survey and to determine whether there might be a better way to frame communication for increasing password length to password users by password administrators. This led to our remaining questions:

Q_2: Do users prefer shorter passwords and are they reluctant to use passwords of 11 characters or more?

Q_3: Do users prefer fewer password changes and are they more willing to use longer passwords of 11 characters if they do not have to change those passwords?

Q_4: Do users have a preference for fewer password changes and are they more willing to add characters to their current passwords if they do not have to change those passwords?

RESULTS

In this section of the paper, we present our findings from both our website study and our user survey. In our web study, our first proposition was that the password protocols posted on websites will have no convergent consensus as to length or duration. If website password requirements conform to theory, then strong passwords policies will require a minimum of 10 or more characters. How well do website password policies conform to these requirements?
To answer this question, we examined the password protocols of 154 organizations whose password-creation requirements could be found on their official websites. One password protocol of interest to us was "password length." Table 1 contains a frequency distribution for the minimum password length required by each website.

Table 1 – Website Minimum Password Length Required

Minimum Length	Total	Percent
Any length (1)	38	25%
2, 3	0	0%
4	4	3%
5	7	5%
6	50	32%
7	8	5%
8	42	27%
9	4	3%
10	1	1%
Grand Total	154	100%

In this table, the modal length was "6" characters, but a substantial number of websites mandated a minimum of "8" characters. Of course, both values are less than the recommended minimum password length of "10." We assigned the value of "1" to password protocols requiring "any length" on the assumption that passwords must be at least 1 character in length. The fact that fully one-fourth of the entire sample had such non-stringent requirements suggests that this same percentage of organizations permit users to create the weakest of passwords—at least in terms of length. Both sets of findings echo those of Furnell (2007) in his ten-website study.
Many of the corporate websites also enabled us to determine the maximum password length allowed. Table 2 summarizes our findings.

Table 2 - Website Maximum Length Specified

Max Length	Total	Percent
6	7	5%
7	1	1%
8	33	21%
9	4	3%
10	2	1%
11	1	1%
12	4	3%
14	3	2%
15	8	5%
16	3	2%
20	5	3%
21-32	7	5%
127	1	1%
any	76	49%
Grand Totals	154	100%

A surprising number of organizations cap their password lengths at "8 characters"—this despite the known fact that passwords of 8 characters are easily cracked and therefore not recommended. We also note that nearly half (49%) of the website policies had no maximum password length—a desirable policy if users voluntarily opt to take advantage of it.

Next, we were interested in how much time users had before they were required to change their passwords. Table 3 provides a summary of these password-changing protocols in our 154-organization sample.
The table makes clear that, while a few website policies require frequent password changes, most do not. In fact, adding the percentages for "any" and "not stipulated" (which we interpret to mean "no requirement"), we found that over half of the

organizations in our sample had no maximum durations. This is interesting given the high percentage of short passwords permitted by most of these websites. The protocol of not changing a password is coupled with the protocol of 10 characters or longer. These two protocols should not be uncoupled—they go hand in hand. If a password profile calls for shorter passwords, they should be changed frequently as these shorter passwords are more easily cracked and therefore represent increased security risks (Cazier & Medlin, 2006; Howard, 2006; Wakefield, 2004)

Table 3 - Website maximum time allowed before a password change is required

Change Protocol	Total	Percent
60 days or less	9	5%
61-90 days	15	10%
4 months	3	2%
6 months	18	12%
1 year	3	2%
"often," regularly," or "when necessary"	16	10%
Any	33	22%
Not stipulated	56	37%
Grand Totals	153	100%

As noted above, we were also interested in the tolerance of end users to various password-protocol requirements. To examine the research questions related to this, we conducted a survey of end users, using the survey instrument shown in Appendix A. We surveyed business students and faculty at four universities in four states, business people from faculty advisory committees, and, to cast a wider net, both local and distant friends. In total, we asked 487 individuals to complete the survey, of which 240 responded for a participation rate of 49%. Within this total, 114 (49%) of the respondents were male and 119 (51%) of the respondents were female, while seven did not answer this gender question.

In the discussions that follow, the total numbers of responses to each survey question differ because not every respondent answered every question in our survey. Table 4 indicates the highest level of education of the respondents. We attribute the disproportionate percentage of master's and doctoral degree holders to the fact that many of our respondents were university instructors.

Table 4 - Highest Level of Education Completed

Answer Options	Response Count	Response Percent
Less than high school	0	0.0%
High school/GED	14	6.0%
Some college	81	34.6%
2 year college(Assoc. Degree)	26	11.1%
4 year college (BA/BS Degree)	38	16.2%
Masters degree	24	10.3%
Doctoral degree	41	17.5%
Professional degree (e.g., MD or JD)	10	4.3%
Grand Totals	234	100.0%

We also asked respondents to provide their occupation. Table 5 details the occupation of participants.

Table 5 - Occupation of Respondents

Occupation	Response count	Response Percent
Student	84	37.3%
Education	54	24.0%
Other	30	13.3%
Retired	24	10.7%
Administrator	7	3.1%
Accountant	5	2.2%
Bookkeeper	3	1.3%
Homemaker	3	1.3%
Self Employed	3	1.3%
Other (each 2 responses or less)	12	5.4%
Grand Totals	225	100%

The lead question of our survey asked the participants to indicate the minimum password length required for all the passwords they use. Table 6 summarizes their responses to this question.

Table 6 - Minimum Password Length Reported

Minimum Length	Total	Percent
0	7	3.0%
4	14	5.9%
5	14	5.9%
6	90	38.1%
7	26	11.0%
8	80	33.9%
9	2	0.8%
10	1	0.4%
11	1	0.4%
12	1	0.4%
Grand Total	236	100.0%

As in Table 1, the modal length was "6 characters" with "8 characters" a close second. Statistically, a matched-pairs test with seven degrees of freedom on these two sets of data showed no significant differences ($p < .07$). These results also suggest that our independent samples are likely to be representative of the population of password protocols from which they were drawn.

The second question of our user survey asked respondents how often they were required to change their passwords. Table 7 summarizes their answers to this question. As in our website survey, nearly half of our respondents indicated that they were never required to change their passwords. Table 7 also indicates that less than 20% of the respondents were required to change their passwords every three months or less. Finally, we performed a chi-square test on the data reported in Tables 3 and 7, but found no statistical relationship between them ($p>.72$).

Table 7 - Maximum time allowed before a password change is required

Frequency	Total	Percent
Never	109	46.0%
Monthly	7	3.0%
Every 3 months	31	13.1%
Every 4 months	5	2.1%
Every 6 months	27	11.4%
Every year	49	20.7%
Other	9	3.8%
Totals:	237	100.0%

Our survey also asked several questions about user password preferences. Question 3, for example, asked users about the longest password they had ever chosen—an indicator of maximum password-length preference. Table 8 summarizes their answers to this question. Assuming that users were not constrained by maximal length restrictions, it seems clear that users prefer short passwords. Looking at the cumulative percent column, for example, the maximum password length chosen by over half the participants in our survey was eight characters or less, and almost 85% of the respondents had limited themselves to 10 characters or less.

A password length of "10 characters" appears to be a threshold value to end users. Accordingly, Question 5 of our survey asked respondents if they would be willing to use an 11-character password if they knew they would be required to change it regularly. The left side of Table 9 summarizes their responses to this question. In short, the results suggest that nearly 80% of users are *not* willing to use such long passwords if they are also required to change them on a regular basis.

Table 8 - Maximum password lengths chosen by users

Maximum Length	Frequency Count	Percent	Cumulative percent
0	15	6.3%	6.3%
4	11	4.6%	10.9%
5	5	2.1%	13.0%
6	26	10.9%	23.8%
7	23	9.6%	33.5%
8	56	23.4%	56.9%
9	32	13.4%	70.3%
10	35	14.6%	84.9%
11	5	2.1%	87.0%
12	14	5.9%	92.9%
13	3	1.3%	94.1%
14	5	2.1%	96.2%
15	2	0.8%	97.1%
16	3	1.3%	98.3%
17, 18, 24, 25	1 each	1.7%	100.0%
Grand Total	239	100.0%	100.0%

Question 7 of our survey asked respondents if they would be willing to use an 11-character password if they were *not* required to change it periodically. As indicated in the right two columns of Table 9, almost 85% of the respondents indicated that they were willing to use such a password length if no changes were required. This high sensitivity to change requirements is important. It suggests what website administrators perhaps already know—users do not like to change their passwords,

but are much more willing to create longer ones if the passwords themselves are "permanent."

Table 9 - Willingness to use an 11-character password

Willingness to use 11 Characters in password	Change required		Change not required	
	Total	Percent	Total	Percent
Yes	47	20.1%	198	84.6%
No	187	79.9%	36	15.4%
Total	234	100.0%	234	100.0%

Lastly, we asked users how many *additional* characters they would be willing to add to their current passwords if (1) they were required to change their passwords periodically (Question 6), or (2) they were *not* required to change their passwords periodically (Question 8). Table 10 summarizes the answers to these questions. In both cases, user preferences were for smaller numbers of additional characters. An additional 3 characters seems to be the users' modal preference. We also note that a higher percent of respondents were willing to add more characters at each level when future password changes were not mandatory. A chi-square test of the two distributions indicates that these differences are statistically significant ($p < .02$). In short, the results of these questions confirm what intuition might suggest—users prefer smaller passwords, but are more willing to use larger ones if they are not required to change them.

Table 10- Number of characters users are willing to add to their longest password

Number of Added Characters	Change Required		Change not required	
	Total	Percent	Total	Percent
3	84	35.9%	94	40.2%
4	22	9.4%	26	11.1%
5	8	3.4%	16	6.8%
6	14	6.0%	27	11.5%
Other	106	45.3%	71	30.3%
Grand Total	234	100.0%	234	100.0%

DISCUSSION

Our (first) sample of website password protocols suggests that most policies permit users to create simple passwords of 6 characters of less. But, overall, we found no consistency here. Thus, our results support our first proposition ($\mathbf{Q_1}$) that the

password protocols posted on websites have no convergent consensus as to length or duration. This surprised us, given the desirability of stronger passwords.

We can make similar comments for the required *durations* of website passwords. About a third of the sites in our sample had no time limits for changing passwords, and only about a quarter of them required users to change their passwords in six months or less. We speculate that the importance of "user-friendly policies" or an absence of critical information at these sites may play roles in such policies. It is also possible that many of the organizations requiring user passwords do so more to protect themselves against liability than to implement true security features. Again, we emphasize that these are only speculations that require further empirical study to confirm or refute.

Our survey of end users also had some interesting revelations. Most of the individuals in our sample preferred shorter passwords, which of course are easier to remember, and over half of these users avoided passwords over 8 characters in length. Passwords of 11 characters or more were virtually nonexistent. We feel that these results therefore support our second question ($\mathbf{Q_2}$) that end users prefer shorter passwords and resist using longer ones.

Until now, the relationship between "password duration" and "password length" has been largely unexplored from an empirical perspective. Are users willing to endure longer passwords if they do not have to change them often? Our study suggests that the answer is "yes." In particular, the results from Questions 5 and 7 of our second study support our third premise ($\mathbf{Q_3}$) that users are more willing to use passwords of 11 characters, provided they do not have to change those passwords.

Finally, the responses from Questions 6 and 8 of our survey suggest that users are more willing to add 3 characters to their current passwords if they do not have to change those passwords— i.e., we found support for $\mathbf{Q_4}$. This last finding may be of particular interest to password administrators who want users to employ longer passwords.

Table 11 summarizes these findings—mainly that we found support for all four of our research premises. These results also have some interesting implications for password administrators. Left to their own devices, for example, end users appear to resist creating large passwords despite the intuitive idea (and empirical evidence) that longer passwords are harder to guess and are therefore more secure. Consequently, where the need for security is high, password administrators should require longer passwords and not depend upon users to implement this control. For the authors, perhaps our biggest surprise was the indication that end users are willing to (literally) go to these lengths if they can keep their passwords for longer periods of time. This seems like a good tradeoff and a win-win situation for administrators of those applications requiring longer passwords.

Table 11- Summary of Results

Propositions		Result
Q_1	Website password protocols will have no convergent consensus as to required password length or duration.	Supported
Q_2	Users prefer shorter passwords and are reluctant to use passwords of 11 characters or more.	Supported
Q_3	Users have a preference for fewer password changes and are more willing to use passwords of 11 characters if they do not have to change those passwords.	Supported
Q_4	Users have a preference for fewer password changes and are more willing to add characters to their current passwords if they do not have to change those passwords.	Supported

Our survey results also suggest that password administrators will find it easier to require users to add 3 or 4 characters to their existing passwords than to ask these same users to create entirely new 11 character passwords. It is also important to couple these long passwords with the password protocol of not requiring users to change these long passwords unless there is a security breach—as long as these are complex passwords.

For IT managers, this might mean fewer password resets and thus more time for security personnel. For users, this could lead to easier password management as a result of fewer mandated password changes. Obviously, any convergence of user password preferences and website password protocols will be of benefit to both groups.

Caveats

The findings presented here are subject to a number of limitations and must therefore be interpreted with care. One concern is the fact that our examination of websites was limited to only those websites that posted those password protocols required of their users—a potentially biased sample. Another concern is the fact that we acquired password data from voluntary participants—another potential source of bias.

A third concern is that we computed our statistics using the self-reported data provided by our respondents. Because we lacked the means to independently verify their answers, we recognize this as a potential problem. This is particularly important for the questions regarding password lengths because we realize that what a respondent *says* he or she is willing to do might not be what he or she would *actually do*.

Finally, we note that, especially in our second study, we did not categorize our results by security level. For example, we would hope that high-level security applications

impose more stringent password protocols on users than low-level ones, or that users would voluntarily opt for such protocols in more-sensitive venues. We did not control for this, nor have previous scholars investigating password protocols. We suggest that this is a fruitful avenue for further research.

SUMMARY AND CONCLUSIONS

The continued popularity of password usage, both in commercial settings and in academia, along with a history of network access breaches, suggests that it is difficult to overstate the importance of password security. To assess password usage in practice, the authors examined the password protocols of 154 websites. Our findings include the following: (1) almost 25% had no minimum password length, (2) nearly 70% of these sites had minimum length requirements of 7 characters or less, (3) 27% of these sites had *maximum* password lengths of 8 characters or less, (4) only 31% of these websites required users to change their passwords in one year or less, and (5) over half the website protocols had no policies requiring users to change their passwords--ever. These findings contrast sharply with the theoretical recommendations for strong-password protocols.

We were also interested in how willing users were to increase their password sizes. A total of 240 individuals voluntarily answered a web-based questionnaire to help us answer this question. Notable findings from this survey were: (1) the modal minimum password length was "6 characters," (2) nearly half the respondents were using passwords that never required changing, and (3) over half the respondents were using passwords of 8 characters or less.

We also found that users were even more sensitive to password-change requirements than to the mandated password lengths themselves. For example, we found that nearly 80 percent of the respondents were not willing to use an 11-character password that required periodic changes, but nearly 85 percent were willing to use one if it did *not* require such change. A similar finding applied to the willingness to add 3, 4, 5, or even 6 characters to their existing passwords—i.e., more users were willing to make such additions if they were *not* required to change the resulting password. These results indicate a divergence between web password policies and user password preferences that should be considered important when developing password policies.

REFERENCES

Barra, R., & Griggs, K. (2007). Internal Controls: Lessons to Be Learned from Fire. *International Journal of Services and Standards, 3*(4), 375-389.

Cazier, J., & Medlin, B. (2006). Password Security: An Empirical Investigation into E-Commerce Passwords and Their Crack Times. *EDPACS, 34*(5), 1-14.

Cole, E. (2001). *Hackers Beware: Defending Your Network From the Wiley Hacker.* Boston: New Riders Publishing.

DeAlvare, A. (1990). *How crackers crack passwords or what passwords to avoid.* Paper presented at the Unix Security Workshop, Portland, OR.

Dixon, P. (1987). The Processing of Organizational and Component Step Information in Written Directions. *Journal of Memory and Language, 26*(1), 24-35.

DOD. (1985). *Password Management Guideline.* Retrieved. from.
FBI. (2002). Password Protection 101. Retrieved September 22, 2002, 2002, from http://www.nipc.gov/publications/nipcpub/password.thm

Florencio, D., & Herley, C. (2007). *A large-scale study of web password habits.* Paper presented at the International World Wide Web Conference - Security, Privacy, Reliability and Ethics, Alberta, CA.

Fordham, D. (2008). How Strong are Your Passwords. *Strategic Finance, 89*(11), 32-47.

Furnell, S. (2007). An Assessment of Website Password Practices. *Computers & Security, 26*, 445-451.

Gaw, S., & Felten, E. W. (2006). *Password management strategies for online accounts.* Paper presented at the Proceedings of the Second Symposium on Usable Privacy and Security, Pittsburgh, PA.

Grampp, F., & Morris, R. (1984). UNIX Operating System Security. *Bell System Technical Journal, 63*(8).

Harthun, K. (2009). Gmail Vulnerability Points Up the Need for Strong Password Policy [Electronic Version]. *IT Knowledge Exchange*, from http://itknowledgeexchange.techtarget.com/security-corner/gmail-vulnerability-points-up-the-need-for-strong-password-policy/

Howard, M. (2006). How Often Should You Change Your Password? *Login, 31*(6), 48-51.

IS Standards, Guidelines and Procedures for Auditing and Control Professionals, (2007).

ISecAuditors. (2009). Gmail vulnerable to automated password cracking [Electronic Version]. *ISecAuditors Security Advisories*, from http://seclists.org/fulldisclosure/2009/Jul/254

Ives, B., Walsh, K., & Schneider, H. (2004). The Domino Effect of Password Reuse. *Communications of the ACM, 47*(4), 75-78.

Kubota, T. (2008). *Cybercrime, Cybersecurity, and Financial Institutions Worldwide.* Hershey, PA: Information Science Reference.

NIST. (2006). Federal Information Processing Standard 201 - Personal Identity Verification of Federal Employees and Contractors. 91.

Ozok, A. A., & Holden, S. (2008). A strategy for increasing user acceptance of authentication systems: insights from an empirical study of user preferences and performance. *International Journal of Business and Systems Research, 2*(4), 343-364.

Prince, B. (2010). Facebook Adds One-Time Password Security Feature to Accounts [Electronic Version], from http://www.eweek.com/c/a/Security/Facebook-Adds-OneTime-Password-Security-Feature-to-Protect-Accounts-890325/

Richmond, R. (2010, October 12, 2010). What to Do If Hackers Steal Your Online Accounts. *New York Times*, from http://gadgetwise.blogs.nytimes.com/2010/09/29/what-to-do-if-hackers-steal-your-online-accounts/?src=mv

Wakefield, R. (2004). Network Security and Password Policies. *The CPA Journal, 74*(7), 6-7.

Walsh, K., Ives, B., Louwers, T., & Schneider, H. (2006). An Exploratory Survey of Password Re-Usage. *Journal of Forensic Accounting, 7*, 237-244.

Webber, J., Guster, D., Safonoy, P., & Schmidt, M. (2008). Weak Password Security: An Empirical Study. *Information Security Journal, 17*(1), 45-54.

Wolfe, D. (2006). Poor Passwords. *American Banker, 171*(240), 5.

Zetter, K. (2010). Hacked Voting System Stored Accessible Password, Encryption Key [Electronic Version], from http://www.wired.com/threatlevel/2010/10/voting-system-hacked/

APPENDIX A - SURVEY INSTRUMENT

Some computer systems enforce a minimum password length while others do not. This survey contains questions about both types of systems.

Minimum Length Password Enforcement
When the computer system *enforces a minimum password length*, what is the required length for this password? (Consider all your passwords—work, school, personal, etc.)
Length _____Put zero if not applicable

How often are you *required* to change this password (Circle the closest alternative)?
Never, Monthly, every 3 months, every 4 months, every 6 months, every year, Other

No Minimum Password Length Enforcement
When *no* minimum password length is enforced by the system (you are free to choose) what is the longest password that you have chosen? (Consider all your passwords—work, school, personal, etc.)

Length _____Put zero if not applicable

How often are you *required* to change this password (Circle the closest alternative)?

Never, Monthly, every 3 months, every 4 months, every 6 months, every year, Other

"What if" Questions
Would you be willing to use an 11 character password if you knew that you would be required to change your password on a regular basis?

Yes, No

How many characters would you be willing to add to your current longest password if you knew that you would be required to change your password on a regular basis?
3, 4, 5, 6, other_____

Would you be willing to use an 11 character password if you knew that you would NOT have to change your password unless it had been compromised?

Yes, No

How many characters would you be willing to add to your current longest password if you knew that you would not be required to change your password on a regular basis?

3, 4, 5, 6, other_____

Profile Questions

Age: <15, 16-20, 21-30, 31-40, 41-50, 51-60, 61-70, >70

Occupation_____

Gender Female _____Male_____

Highest Level of Education Completed:

Less than high school, high school/GED, some college, 2 year college (Assoc. Degree), 4 year college (BA/BS Degree), Masters Degree, Doctoral degree, Professional degree (e.g., MD, JD)

Roberta Ann Barra worked for a decade in public, private, and governmental accounting before pursuing a career in academia; holding positions as a Controller and a Fiscal Manager and consulting on accounting software installation projects involving accounting and ERP software. She holds an MBA from the University of Houston and a Ph.D. from the University of Illinois at Champaign-Urbana. Currently teaching and conducting research at the University of Hawai'i at Hilo, Dr. Barra has held positions at the University of Texas at Arlington, California Polytechnic State University at San Luis Obispo, and Pittsburg State University in Pittsburg, Kansas. Her research has focused on Fraud and Information Systems including controls, software evaluations, and documentation techniques.

Alexander McLeod is an Assistant Professor of Information Systems at the University of Nevada, Reno. He received his Ph.D. in Information Technology from the University of Texas at San Antonio. His research in information system security, healthcare information systems, tax and technology and enterprise systems appear in over 20 journal articles.

Arline Savage is Professor of Accounting and Deloitte Faculty Fellow at California Polytechnic State University, San Luis Obispo. She received her doctorate from the University of Port Elizabeth (now Nelson Mandela Metropolitan University) in South Africa. Her areas of expertise are Financial Reporting, Financial Analysis, Forensic Investigations, and Information Systems. She has over 35 peer-reviewed publications.

Mark G. Simkin is a professor of Information Systems at the University of Nevada, Reno (simkin@unr.edu, College of Business/026, University of Nevada, Reno, Nevada, 89557, USA). He earned his MBA and Ph.D. degrees from the University of California, Berkeley. His research in end-user computing, computer education, and

computer learning appears in over 100 academic journal articles, including Decision Sciences, The Decision Sciences Journal of Innovative Education, The Journal of