Journal of Information Technology Management

ISSN #1042-1319

A Publication of the Association of Management

A DEVELOPMENTAL PERSPECTIVE ON WEAK PASSWORDS AND PASSWORD SECURITY

JAMES E. WEBER
ST. CLOUD STATE UNIVERSITY
jweber@stcloudstate.edu

DENNIS GUSTER
ST. CLOUD STATE UNIVERSITY
guster@stcloudstate.edu

PAUL SAFONOV
ST. CLOUD STATE UNIVERSITY
safonov@stcloudstate.edu

ABSTRACT

In this study, 273 subjects were instructed to devise passwords that they might use for an important purpose, then asked how they had developed those passwords. The passwords developed were evaluated according to their complexity and adherence to strong password development standards, then were subjected to attack from a standard hacker tool. Results indicated generally weak passwords were developed. In contrast to best practices, passwords developed were overwhelmingly related in some way to the developer of the password. Implications for the development of strong passwords, and for further research and practice are discussed.

Keywords: passwords, password development, weak passwords, strong passwords, mnemonic passwords.

INTRODUCTION

Password users are faced with a dilemma. Password security is an increasingly important part of modern life, but the number of passwords each person has to manage has increased dramatically. With the increase in internet e-commerce sites, some people are managing as many as 15 different passwords (Ives, Walsh, and Schneider [9]). Users, faced with cognitive limits of processing and recall (Miller [12]; Warkentin, Davis, and Bekkering [23]) are developing weak passwords that don't provide proper security (Bort [2]; Cazier and Medlin [3]; Fontana [7]; Ives et al. [9]; Mulligan and Elbirt [13]; Kelly [11]; Stanton, Stam, Mastrangelo & Jolton [18]; Wakefield [22]). The problem of developing passwords that are simultaneously secure and easy to remember is a difficult one for users (Bort [2]). In fact, weak or nonexistent passwords are rated as the top 10 computer vulnerabilities by the SANS (SysAdmin, Audit, Network and Security) Institute [16]. Although alternatives have been suggested, including biometrics and two factor authentication, problems with acceptance, cost and implementation mean that for the foreseeable future passwords will remain the primary method used for authentication purposes (Bort [2]; Fontana [7]).

Anecdotal evidence of poor password practice such as passwords written on post-it notes and stuck to the user's computer, or passwords consisting of the word "password", the users birthday, or even the users name are easy to find (Engebretson [5]; Piazza [15]; Thurm & Mangalindan [20]; Tuesday [21]). Passwords such as these provide weak security and are susceptible to social engineering (Blundo, D'Arco, DeSantis & Galdi [1]; Semjanov [17]; Wakefield [22]; Warkentin et al. [23]). It has been variously estimated that between 15% and 50% of such passwords can be cracked (Kelly [11]; Tuesday [21]). The security industry has responded with software that can be used to detect weak passwords (Blundo et al. [1]), but users are still left with the problem of developing and recalling strong, more complex passwords (Miller [12]; Warkentin et al. [23]).

The precise definitions of strong and weak passwords are in a state of constant flux as changes in technology render them obsolete. In general though, weak passwords are those that are easily compromised, either through guessing, brute force attacks, hacking or attacks that pre-compute hashes of possible passwords and compare them against stolen password files. A strong password is one that takes longer to crack than the password change interval. At this point in time, a strong password might be thought of as consisting of at least 8 characters, multiple upper and lower case letters, numbers, and multiple special characters (Thomas [19]). Experts differ on how strong a password is, with Tuesday [21] indicating that a stolen encrypted password might be cracked by a low-end hacker within a few days and others indicating that all encrypted passwords can be cracked within 45-60 days (Thurm and Mangalindan [20]).

In general, password strength increases as the password becomes longer and more complex, or includes multiple numbers letters and different kinds of characters. Certain types of passwords, however, are automatically considered to be weak. Words and numbers are easily cracked regardless of length, and names, initials, pets, friends, etc. are too easily "socially engineered". Different methods have been suggested to help users develop and remember strong passwords. One suggestion is a "password phrase" that is both easy to remember and easily translated into a combination of letters, numbers and symbols by taking the first letters of each word and substituting numbers and special characters into appropriate spots (DeLisser [4]; Flandez [6]). The phrase "Easy for you to say!" might be translated into EZ4U2Say! in this way. There are several similar alternatives to this process (Thomas [19]) and research has shown that these mnemonic passwords are as easy to recall as naïve passwords (Piazza [15]).

As passwords have become stronger, hackers have turned their attention to weak passwords. Social engineering and standard hacker tools are used to attack weak passwords by hashing a dictionary of possible passwords, then comparing the hashes to the stolen passwords (Semjanov [17]). Commercial services are available that do much the same thing (Password Crackers [14]) and hackers programs that concentrate on weak passwords using the easy availability of computing power have put password cracking within the reach of even the casual hacker.

In evaluating passwords, it has become increasingly important to evaluate not only how complex the password is, and therefore resistant to brute force cracking attacks, but how the password was developed by the user. A seemingly random password that is consists of initials and an anniversary date is much easier to crack than would be evident from a visual inspection of the password.

THIS STUDY

In this study, 273 business students enrolled at a mid-sized Midwestern university were surveyed regarding password development practices. Students were viewed as an appropriate sample for a number of reasons. First, students face the same cognitive limitations (Miller [12]) as business employees in trying to recall passwords, and they will soon carry their password habits into the workplace. Today's students are also extremely busy balancing work, school and a social life, thus facing time constraints similar to employees in business. Finally both students and many employees face a lack of private work space, making "social engineering" of passwords written on post-it notes or notebooks possible.

In addition to items concerning standard demographic information, the survey asked subjects to devise a password that they would use for an important purpose like accessing their bank account online. Subjects were also asked how they developed this password, along with several single-item measures regarding awareness of computer security issues. Based on research by Frank, Shamir & Briggs [8], it was expected that subjects that were more aware of computer security issues would develop passwords in a more sophisticated manner.

Researchers coding the data included a field that identified words, numbers, names or acronyms based on the researchers' visual inspection of the data. In addition, a complex coding system was developed to reflect how subjects related that they had developed these passwords and this coding system was used categorize data during data entry. The coding system included four major catego-

ries of passwords, three minor categories, and 65 subcategories. The vast majority of all passwords used by subjects fell under the four major categories, number related and related to the subject, word related and related to the subject, name related and related to the subject, or randomly developed. Throughout this paper, researchers will refer to these categories simply as numbers, words, and names, leaving out the explanation that these passwords are related in some way to the subject. Finally, researchers developed a measure of password complexity and all entries were coded to reflect this evaluation.

In terms of password complexity, if a password is comprised of a single character and only lower case letters, only 26 options need to be considered in guessing the password. If the single character password is comprised of only numbers, 10 options would need to be considered in guessing the password. If a password is four characters long and comprised of both cases of letters and numbers, each character in the password has 62 possible values. The total number of different passwords that can be made up of these combinations is 62 to the 4th power, or 14,776,336 different combinations. In the researchers' measure of password complexity, the number of possible combinations in the password is expressed in scientific notation and the exponent used as the coding measure. In this example, the exponent would be "7" and the password coded as a "7" for password complexity. An eight-character password that contains numbers, special characters and both cases of letters would receive a complexity score of 15 using this method. This type of password fulfills the minimum recommended requirements of the SANS Institute in their Security Policy Project [16]. Password complexity ratings in this study varied from a low of four to a high of 29.

The passwords provided by subjects were hashed using two different hashing algorithms commonly available in UNIX. The first algorithm used, DES (Data Encryption Standard) is a 64-bit cipher that is now typically used in situations not requiring the highest level of security. The other algorithm, MD5 (Message Digest 5, sometimes referred to as MD5Sum), provides 128 bit encryption for situations requiring greater security.

The resulting hashes were run through a common, downloadable password cracker, John the Ripper [10] on a Linux based 16-processor computer cluster. The hashes were run through twice, once using a basic cracking dictionary consisting of about 45,000 common English words and names. The second time through a simple routine to identify numbers was used. The results of whether a password was cracked during this "hack-attack" were then coded and entered into the researchers' database.

Researchers were interested in investigating a number of questions related to password development, complexity and security. The password cracker that was employed checked numbers, common words and some common names. One issue was whether the passwords were cracked consistent with the researchers' coding of passwords into numbers, words and names based on visual inspection. In order to address this issue, the percentage of passwords cracked in each category was calculated, the passwords that were cracked were compared to the categories of passwords coded by visual inspection of the researchers, and discrepancies were resolved. In order to further clarify the issue, ANOVA was run to check whether the passwords that were cracked differed in password complexity from those that weren't cracked. In this analysis, password complexity was the dependent variable and whether the password was cracked or not was the fixed factor.

Researchers were also interested in how subjects' awareness of computer security issues might be related to how the subjects developed passwords. Those with greater awareness of computer security issues were expected to be more likely to develop random passwords. For this analysis, subjects were divided into two groups according to whether they developed a password at random or if they developed the password based on a number, word or name related in some way to themselves or those close to them. The 14 subjects who couldn't be classified in one of these categories were dropped from this analysis. This random versus nonrandom password development was then used as the fixed factor in an ANOVA while awareness of computer security issues was used as the dependent variable.

Also of interest was whether password complexity varied according to how subjects developed passwords. Subjects were divided into four groups according to whether the password developed was number related, word related, name related or random. To explore this question, ANOVA was run with the type of password development as the fixed factor and password complexity as the dependent variable.

Finally researchers looked to see if there was a relationship between whether a password was cracked or not and how the password had been developed. The four-group password development variable used above was used as one nominal variable, while whether the password was cracked or not was used as another. The SPSS procedure "Crosstabs" was used to investigate the nature of the relationship between these two nominal variables.

RESULTS

The password cracker running on a 16 processor Linux cluster took three seconds to process the password file encrypted using DES and 10 minutes and 48 seconds to process the file encrypted using MD5Sum. The same passwords were cracked in each case. Of the 273 passwords submitted to the password cracker, 79 or 28.9% were cracked. This compares with 89 numbers, words, names and acronyms identified by the researchers during data entry. Researchers had coded one acronym, two names (both variants of female first names) and seven words (all foreign words) that were apparently not within the 45,000 entries in the cracker dictionary. Table 1 shows the breakdown of cracked passwords. Results showed that passwords susceptible to cracking by the program used in this study were generally easily identifiable by visual inspection.

Table 1: Characteristics of Cracked Passwords

Password Type	Number	Percent
Numbers	51	64.6
Words	25	31.6
Names	3	3.8
Total	79	100

Although the percentage of passwords cracked is unacceptably high, it falls within the estimates of Kelly [11] and Tuesday [21] that between 15 and 50% of passwords can be cracked. Table 2 shows information on the password complexity measure developed by researchers for the passwords examined. It should be noted that the most complex password cracked had a password complexity rating less than the 15-value of a SANS recommended password.

Table 2: Complexity of 273 Passwords Cracked and Not Cracked by the Password Cracker

	N	Minimum	Maximum	Mean	Std. Dev.
Cracked Passwords	79	4	13	7.10	2.38
Uncracked Passwords	194	6	29	13.40	3.87

ANOVA was used to assess the variability of password complexity by password cracking. The significant relationship F(1, 271) = 180.84, p = .000, between password complexity and whether the password was cracked or not is evident from the results shown in Table 3. The results are instructive given that the cracker essentially picks out all words, names and numbers. It shows that passwords that were cracked were also significantly less complex than those not cracked.

Table 3: ANOVA, Password Complexity by Whether the Password Cracked

Password was	N	Mean	Std. Dev.	F	Sig.	Power a
Cracked	79	7.10	2.38	180.84	.000	1.000
Not Cracked	194	13.40	3.87			
Total	273	11.58	4.53			

a Observed Power, alpha = .05
R squared = .400

A weaker relationship existed between awareness of computer security issues and the development of strong, random passwords (F(1, 257) = 6.076, p=.014). For this analysis, subjects who developed passwords related to numbers, words and names were grouped together, as opposed to those subjects who developed random passwords. The 14 subjects who couldn't be classified in this way were dropped from this analysis. Results of an ANOVA with awareness as dependent variable and random or nonrandom password development as the fixed factor are presented in Table 4. As the Table 4 shows, although a significant difference exists in the awareness of security issues between those who developed the stronger, random passwords and those who developed nonrandom passwords, observed power of the F statistic is only .690 and the R square is equal to only .023.

Table 4: ANOVA, Awareness of Security Issues by Type of Password Development

Password Type	N	Mean	Std. Dev.	F	Sig.	Power a
Random Password	30	4.40	.621	6.076	.014	.690
Nonrandom Password	229	3.97	.929			
Total	259	4.02	.908			

a Observed Power, alpha = .05
R squared = .023

Password complexity also varied significantly according to the type of password developed ($F(3, 255) = 26.098$, $p=.000$). In this analysis, the four major categories of password development processes formed the grouping variable and password complexity was the dependent variable. As shown in Table 5, the primary difference in mean password complexity occurs in the numbers category. An examination of confidence intervals around the means shown in Table 5 show that only the numbers group is distinctly separated from the other groups. This is somewhat unexpected, as the password complexity of randomly generated passwords was not significantly different from words and names, based on an examination of confidence intervals. In addition, analysis shown above in Table 3 had indicated that password complexity impacted whether the password was broken. For these two things to be true simultaneously, numbers, names, words and randomly developed passwords must be broken at different rates.

Table 5: ANOVA, Password Complexity by Type of Password Development

Password Type	N	Mean	Std. Dev.	F	Sig.	Powera
Numbers	57	7.53	4.19	26.098	.000	1.000
Words	77	13.06	3.59			
Names	95	12.51	3.84			
Random	30	11.93	4.26			
Total	259	11.51	4.43			

a Observed Power, alpha = .05
R squared = .235

In order to investigate whether the type of password development process was associated with whether the password ended up being cracked, Crosstabs and a chi-square statistic were utilized. Table 6 shows the Pearson chi-square results indicating that different types of password development resulted in passwords that were cracked at a different rate ($\chi 2 = 100.436$, $df=3$, $N=259$, $p=.000$). Passwords related to numbers or words were more likely than expected under the null hypothesis to be cracked, while passwords related to names and randomly developed passwords were less likely than expected to be cracked. Cramer's V equaled .623, indicating a relatively large difference between expected and observed values. Since the standard hacker's dictionary included approximately 45,000 words and was augmented with a routine that checked numbers, these results confirm that the password cracker worked as expected and support conclusions drawn above. As researchers examined Table 6, they were surprised to see that two passwords that subjects described as having been developed at random had been broken by the password cracker. An examination of the dataset revealed that these passwords that were described as having been developed at random were actually numbers. The simple routine used in this study to crack numbers easily cracked these passwords.

Table 6: Chi-Square Analysis of Type of Password Development by Whether the Password was Cracked

		Type of Password Developed					
Password was	N	Number	Word	Name	Random	Chi-Square	P
Cracked	76	46	20	8	2	100.436	.000
Not Cracked	183	11	57	87	28		
Totals	259	57	77	95	30		

DISCUSSION

Perhaps the most striking finding to come from this study is that the great preponderance of subjects developed passwords that were in some way related to them self. In the survey subjects were asked to explain how they came up with the password that they gave. As researchers developed categories for these explanations, four major ways of developing passwords emerged. The first category, comprised of a minority of 30 subjects, included those who indicated that the passwords were developed at random. For the next three major categories, subjects in-

dicated that they developed passwords that were in some way related to themselves, by either focusing on numbers, words or names. There were a considerable variety of subcategories for each of these major categories. In addition, these categories often included the addition of another of the major categories to the basic password development process. In total, 229 of the 273 subjects who responded to this question developed passwords that could be associated with one of these three major categories. Examples included all sorts of birthdates, anniversaries, phone numbers, etc. for numbers, nicknames, pets names, significant others, relatives, etc. for names, and what the subject typically drove, drank, wore, was described as, etc. for words. Often a nickname was joined with a birth date, or a number with initials, etc. 14 reasons were difficult to categorize, but of the remaining 259 subjects, 229, or over 88% developed passwords associated with some aspect of their lives as described above. Though these passwords could seem random on casual inspection, they were not, thus posing a greater risk from social engineering than randomly developed passwords.

Cracking passwords can take one of two approaches. The brute force method simply tries all possible combinations of relevant elements. This approach is extremely intensive computationally, and is beyond the reach of casual hackers. The other approach is to limit cracking attempts to the most likely candidates; most likely numbers, words from a dictionary or names that may have a relationship to the password user. This is the approach taken by most crackers and is the approach taken in this study.

Still, the measure of password complexity developed by the researchers was useful in differentiating between weak and strong passwords. Passwords that were cracked were rated as substantially less complex than those not cracked. When the password complexity measure was applied to the recommended minimum password standards from SANS, the result was a complexity rating of 15. None of the passwords cracked by the password cracker, even the numbers, were rated that highly. In part that was due to chance. If subjects had used a 15 digit number or a 11 letter word as a password, these would have been scored a 15 on complexity and presumably would have been cracked.

Although awareness of computer security issues was related to the development of stronger, more complex passwords in this study, the relationship wasn't a strong one. Prior research by Frank et al. [8] had suggested that computer related user behavior varied with increased awareness of issues. The significant but small effect size found in the current study was disappointing. More research is needed to determine what leads to the development of stronger passwords. Of particular interest might be an investigation of training in password security and techniques for developing strong passwords, since business provides training routinely for employees.

In terms of password complexity, passwords consisting of numbers were significantly less complex than passwords related to words, names, or randomly developed passwords. This is probably true for several reasons. Since each character in a number has fewer possible values than either letters or special characters, numbers provide the least possible password complexity for any given password length. In addition, subjects often used PINS and other short meaningful numbers like birth dates or anniversaries as the basis for their passwords, leading to shorter overall length passwords when numbers were used. Since all numbers that subjects used as passwords were cracked by the password cracker, selection of a number was a particularly poor way to develop a password.

Although the mean password complexity for words, names and randomly developed passwords in this study could not be said to differ, none of the randomly developed passwords that weren't numbers were cracked while 77 of the other passwords were. The short interval needed to run each password file on the Linux cluster points out how easy it has become to crack those naïve or weak passwords. A larger, more complete dictionary would have cracked perhaps 10% more of the passwords, based on the researchers' visual inspection of the passwords. Additionally, a more sophisticated approach using knowledge of the user's personal characteristics would crack even more. Taken together, the results of this study point to a need for stronger, randomly developed passwords. More research is needed into methods for the development and recall of random passwords. Some suggestions have been offered (DeLisser [4]; Flandez [6]; Piazza [15]; Thomas [19]; Warkentin et al. [23]) but more information is needed on how to develop easy to remember, strong, random passwords. At some point in the future biometrics and forms of multiple-factor authentication will render the problem moot, but until that time there continues to be a need for strong passwords and a means to develop and recall them.

REFERENCES

[1] Blundo, C., D'Arco, P., De Santis, A., and Galdi C. "HYPPOCRATES: a new proactive password checker," *The Journal of Systems and Software,* Volume 71, Numbers 1-2, 2004, p.163.

[2] Bort, J. "Identity management begins with the simple password," *Network World,* October 21, Volume, Number 42, 2002, pp.8-10.

[3] Cazier, J.A., and Medlin, B.D. "Password security: An empirical investigation into E-Commerce Passwords and their crack times," *Information Systems Security*: *The (ISC)2 Journal*, Volume 15, Number 6, 2006, pp.45-55.

[4] DeLisser, E. "Tricks of the trade: A techie's password," *The Wall Street Journal*, May 22, 2002, D1.

[5] Engebretson, D.J. "3 ways to keep passwords and user names out of the wrong hands," *Security Distributing & Marketing,* Volume 34, Number 10, 2004, pp. 39-40.

[6] Flandez, R. "Tricks of the trade: A techie picks a password," *The Wall Street Journal*, October 13, 2004, D1.

[7] Fontana, J. "Chevron has had it with passwords," *Networkworld,* Volume 22, Number 43, 2005, pp.1, 14.

[8] Frank, J., Shamir, B., and Briggs, W. "Security-related behavior of PC users in organizations," *Information & Management*, Volume 21, Number 3, 1991, pp.127-135.

[9] Ives, B., Walsh, K.R., and Schneider, H. "The domino effect of password reuse," *Communications of the* ACM, Volume 47, Number 4, 2004, pp.75-78.

[10] "John the Ripper password cracker," Openwall Project, 2005. http://www.openwall.com/john (accessed 10 April, 2006).

[11] Kelly, C.J. "The password is: Useless (probably)," *Computerworld*, Volume 38, Number 49, 2004, p.32.

[12] Miller, G.A. "The magical number seven, plus or minus two: Some limits on our capacity for processing information," *Psychological Review*, Volume 63, 1956, pp.81-97.

[13] Mulligan, J., and Elbirt, A.J. "Desktop security and usability trade-offs: An evaluation of password management systems," *Information Systems Security: The (ISC)2 Journal*, Volume 14, Number 2, 2005, pp.10-20.

[14] Password Crackers, Inc., "Password Portal - Password Recovery, Password Cracking," 2004. http://www.passwordportal.net (accessed 3 April 2006).

[15] Piazza, P. "Better passwords made easy," *Security Management*, Volume 48, Number 8, 2004, p.34.

[16] *SANS Security Policy Project*, SANS Institute, 2006, http://www.sans.org/resources/policies (accessed 11 April, 2006).

[17] Semjanov, P. "Password Cracking FAQ", 2006. http://www.password-crackers.com/en/articles/12 (accessed 3 April, 2006).

[18] Stanton, J.M., Stam, K.R., Mastrangelo, P., and Jolton J. "Analysis of end user security behaviors," *Computers & Security*, Volume 24, Number 2, 2005, p.124.

[19] Thomas, B. "Information security with minimal training, and without costly infrastructure changes," SANS Institute, 2005. http://www.sans.org/rr/whitepapers/authentication/1636.php (accessed 10 April, 2006).

[20] Thurm, S., and Mangalindan, M. "Trying to remember new passwords isn't as easy as ABC123," *The Wall Street Journal*, December 9, 2004, A1.

[21] Tuesday, V. "Bad policy makes for weak passwords," *Computerworld*, Volume 37, Number 48, 2003, p.38.

[22] Wakefield, R.L. "Network security and password policies," *The CPA Journal*, Volume 74, Number 7, 2004, p.6.

[23] Warkentin, M., Davis, K., and Bekkering, E. "Introducing the check-off password system (COPS): An advancement in user authentication methods and information security," *Journal of Organizational and End User Computing"*, Volume 16, Number 3, 2004, pp.41-58.

AUTHORS BIOGRAPHIES

Dr. Dennis Guster is Professor of Business Computer Information Systems and Director of the Business Computing Research Laboratory at St. Cloud Stat University, MN, USA. His interests include network design, network performance analysis and computer network security. Dennis has 25+ years of teaching experience in higher education and has served as a consultant and provided industry training to organizations such as Compaq, NASA, DISA, USAF, Motorola, and ATT. He has published numerous works in computer networking/security and has undertaken various sponsored research projects.

Dr. Paul Safonov is Assistant Professor of Business Computer Information at St Cloud State University, MN, USA. He obtained his Ph.D. in Applied Mathematics from Russian Academy of Sciences, Moscow, in 1995. Paul's research interests include computer modeling, as well as decision support systems, internetworking and security. He has over 20 years of research experience in Russia, Germany, Belgium, Brazil, France, USA. Paul authored and co-authored over 50 scientific publications, organized and participated in numerous international conferences and sponsored research projects.

Dr. James Weber is Professor of Management at St Cloud State University, MN, USA., where he teaches Strategic Management, Organizational Behavior and International Management. He received his Ph.D. in Business Management from New Mexico State University in 1996, with a minor in International Business. His research interests lie at the intersection of technology and human behavior. His research findings have appeared in a number of leading journals, including the Journal of Computer Information Systems, the Journal of Business Ethics, the Journal of Business Inquiry, the Case Research Journal and the Leadership and Organizational Development Journal among others.