Journal of the Nigerian Association of Mathematical Physics
Volume **19 (November, 2011), pp 483 – 486**

Appraising the Strength of Users Passwords in Computing Systems in Nigeria

Annie. O. Egwali

Department of Computer,
University of Benin, P.O. Box 1154, Edo State, Nigeria.

Abstract

The increases in computerized mode of operations and the activities of identity attackers have not only affected the trust in computerized systems but have slowed down the adoption of both offline and online services. Today there is the risk of unauthorized access, fraud and inappropriate disclosure of sensitive data. Human resources and malicious applications steal user identity, potentially resulting in a direct loss of highly sensitive information and hard currency to affected victims. To protect sensitive information, commercial and corporate sites extensively employ the use of textual passwords, which when used over an encrypted connection is vulnerable to attacks. To counter some of these attacks, many corporate sites instruct users to make use of mnemonic passwords without carefully considering the implications. This paper describes the generation of a novel mnemonic password dictionary, and an empirical study performed to analyze the strength and effectiveness of regular passwords and mnemonic passwords. Findings revealed that users' context, which allows the deployment of mnemonic strategies for password memorization, is prosaic in nature and susceptible to human attackers and automated tools. Commercial and corporate sites will need these findings in order to adopt effective authentication strategies for logging users into their sites.

1.0 Introduction

The "password problem," as formulated by Birget et al [1] and as posited by Wiedenbeck et al [2], arises because passwords are expected to comply with two conflicting requirements, namely:

1. Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans.
2. Passwords should be secure, i.e., they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text.

Meeting these conflicting requirements has proved to be very challenging to humans, and these usability challenges tend to translate directly into security problems ([1]). Several studies and empirical analysis have been conducted on user passwords to determine the strength of passwords against attacks. Yan et al [3] conducted a study with 400 students, and evaluated the security and memorability of regular passwords (RPs), mnemonic passwords (MPs) and random passwords and concluded that MPs are much stronger than RPs and as strong as random passwords. However, their analysis relies on a standard (non-mnemonic) crack dictionary to measure the strength of MPs. Petrie [4] collected 1,200 employees passwords in the United Kingdom and concluded that people select passwords that represent themselves. Adams and Sasse [5] concluded that users lack motivation and do not have an understanding of password policies. Weirich and Sasse [6] performed two studies, to analyze user's attitudes toward strengthening password management. Findings revealed that users do not understand and comprehend their levels of vulnerabilities when authenticating using the password model.

2.0 Password Algorithm

RPs and MPs are scored based on the password algorithm [7, 8, 9], for which the passwords score S is derived by computing the number of characters in the password (Nc) and the character complexity (Ch_n) (e.g. $Ch_n = 26 + 26 + 10 = 62$), which is determined by the number of different character sets (lower-case characters English alphabet (26), upper-case characters English alphabet (26), numbers (10) and the 33 symbols (*, @, #, %, $, e.t.c.)) incorporated into a password. The algorithm is used to compute scores for words not in dictionary, but for words found in the dictionary the score value is zero (0).

Corresponding authors: E-mail: egwali@yahoo.com, Tel. +2347033247730

$$S = \begin{cases} Log_{10}((Ch_n)^{Nc}) \\ 0 \end{cases}$$

3.0 Mnemonic Password Dictionary Generation

To generate MPs for the dictionary, familiar and famous expressions were compiled and a number of techniques were employed. First each word in the expressions is replaced with the character and digit that is phonetically equivalent. Table 1 contains a sample of expressions and their mnemonic equivalent. For example, "To" is substituted with the mnemonic equivalent "2", "Be" with "B", "Your" with "Ur" e.t.c.

Table 1: Words and character/digit equivalent in the MP dictionary.

Words	Character or digit substitution
To	2
Be	B
Your, you are, you're	Ur
The	D
At	@
Four, fore, for	4
You	U
Yahoo.com	Y.com

Next, variations were introduced by replacing a particular character or digit with more than one type of word this is represented in Table 2. For example, the expression "Ignorant is not an excuse for breaking the law" is substituted with the mnemonic password "Iisnae4bdL",the expression "You have to see me at four" is substituted with the mnemonic password "Uh2cm@4 ". In these cases, the original expressions can always be derived from the expressions context if need be.

Table 2: Examples of expressions and equivalent MPs.

Phrase	Mnemonic password
Beauty is in the eyes of the beholder	Biideyesodb
Ignorant is not an excuse for breaking the law	Iisnae4bdL
Give to others what you want others to do to you	G2owUwO2g2U
You have to see me at four	Uh2cm@4
That which is yours cannot be taken away	d@twiurc'tbta
Cough your cough and I will cough my cough	CUrC&I'lCmC

Permutation was also applied by interchanging upper and lower case letters as represented in Table 3 (i.e. ''Oluwatosin'' would also be analyzed as ''OluWaTosin" , "oluwaTosiN'') and altering some letters to numbers within the word string (i.e. Bosede would also be accessed as "B0sede" by changing alphabet "o" to number "0")).

Table 3: Generated MPs Dictionary Contents

Dictionary	Samples
Common names	Stella, Oluwat0sin, 0luwa2sin, Bridget, Mathew, Uwadia, Cynthia, Princewill, ChukWu, Akinola, Ifeanyi, James, Ehimah, 2bena, T0bena
Titles	WafErian, Arrow, Novice, N0vice, maSter, SiSter, yokozuna
Abreviations	Uniben, unilag, rovgbiv
Sports	Barcelona, Manchester, Chelsea, Drugba, Arsenal
Places	Niger, Benin, Lokoja, Abiekuta, LaGos, Sapele, Waffi, BUca
Numbers	2000, twenty,

4.0 Experiments

Over 39055 passwords and expressions were collected including words from the King James Version bible and paired words concatenated to form expressions. Sample set of 324 RPs and 324 constructed MPs with words from expressions were derived from participants. The words from the expressions were later substituted with characters and digits that were phonetically similar to them to create MPs. These were then cracked by comparing them with the generated MP dictionary. In the search, duplicated words were eliminated. Thus a word like "Precious" is considered only once depending on the dictionary it appears though it can be viewed as a name for both sexes and also as a lexicon word. The search also takes into consideration the number of related passwords regardless of the permutation applied to it by a user. Consequently, if the word ''Osase'' is in the dictionary, other passwords like "Esosa", EsAso", EsOaS, etc. will be matching passwords. The effectiveness of user's choices of MPs was also evaluated by analyzing the quantitative value of users MPs when compared with the generated MPs dictionary.

Table 4: Cracked Passwords from a Sample set of 324 RPs and 324 MPs

Dictionary Words	Dictionary Size	Duplicated Passwords	Search Size	Cracked Passwords	Percentage Cracked
Common Names	1101	57	1044	26	4.0
Titles	113	21	92	08	1.2
Celebrities	93	19	74	05	0.8
Uncommon names	1265	81	1184	13	2.0
Numbers	391	21	370	11	1.7
Sports	164	32	132	06	0.9
Character sequences	504	23	481	07	1.1
Bible words	13012	4797	8215	14	2.2
Place names	1249	19	1230	11	1.7
Expressions	623	101	522	68	10.5
MPs	623	0	623	56	8.6
Vulgar words	285	23	262	08	1.2
Dictionary	19632	2013	17619	18	2.8
Total	39055	7207	31848	251	38.7%

5.0 Experimental Results

Table 4 contains the dictionary size of the different dictionary words. From users RPs and MPs collated, after classification under the different dictionary words, duplicated passwords were disclosed and subtracted from the dictionary size to derive the search size. The table also shows the number and percentages of cracked passwords. Findings from passwords cracked from a sample set of 324 RPs and 324 MPs making a total of 648 passwords using the generated dictionary size of 39055 RPs and MPs. Removing duplicated words (i.e. uncommon names like Monday, which stand for a name and one of the days of the week); reduce the data search space to 31848 words and expressions. A total of 251 passwords were compromised representing 38.7%. Although this is a bit low, it reveals the advantage of an attacker if a known dictionary exist for users RPs and MPs. Of the 324 RPs collected, 127 were compromised representing 39.2%. For MPs 124 (38.3%) of the 324 collected were cracked, thus more RPs were cracked than MPs. At closer inspection, it was discovered that the difference in cracked RPs and MPs is minute revealing the fact that MPs are becoming as susceptible as RPs. This is a big contrast from initial results gotten from similar analysis ([10, 3]).

Table 5: Password Strengths

Factors	RPs		MPs	
	Strongest	Weakest	Strongest	Weakest
Nc	14.1	8.3	19.3	9.1
Ch_n	3.2	1.4	4.8	1.3
S	16.2	6.9	18.1	7.4

The strength of users regular passwords and mnemonic passwords analyzed using the password algorithm revealed that generally the mnemonic passwords utilized had increased length (Nc) when compared with regular passwords (see Table 5). Also the character complexity Ch_n was stronger for mnemonic passwords, which reveals that creating longer and more complex passwords based on mnemonic conception increases the strength (S) of passwords ([11]).

6.0 Conclusion

This study makes known the susceptibility of present RPs and MPs to attacks. Previously it was assumed that MPs will be stronger than PRs because firstly, they do not appear in any password cracking dictionary, secondly, the expressions help users incorporate different character classes and thirdly, because the space of possible expressions is virtually infinite. Findings revealed that although users' context allows the deployment of MP strategies for password memorization and MPs are more resistant to brute force attacks as compared to RPs, however as time progresses MPs could become more vulnerable to attacks with the generation of mnemonic password cracking dictionaries, which is still at its early developmental stage. Therefore the utilization of MPs, should not be regarded as the ultimate solution to the password dilemma.

7.0 Reference

[1]. Birget J.C., Hong D. and Memon N. 2006. Graphical passwords based on robust discretization", IEEE Transactions on Information Forensics and Security 1(3) pp. 395-399.
[2]. Wiedenbeck S., Waters J., Birget J. C., Brodskiy A. and Memon N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system, International Journal of Human-Computer Studies, 63: 102-127.
[3]. Yan, J., Blackwell, A., Anderson, R., and Grant. A. 2004. Password memorability and security: Empirical results. IEEE Security and Privacy, 2, (5) pp. 25 - 31.
[4]. Petrie H. 2005. Password clues. http://www.centralnic.com/news/research.
[5]. Adams A. and Sasse. M. A. 1999. Users are not the enemy. Commun. ACM, 42, (12) pp. 40 - 46.
[6]. Weirich D. and Sasse. M. A. 2001. Persuasive password security. In Proc. of Ext. Abstracts CHI 2001, pp. 139 – 140.
[7]. Mac OS X. 2006. Password Assistant. "Passwords: Safety in Numbers." http://www.apple.com/macosx/tips/password13.html
[8]. Mozilla Corporation 2006. http://www.mozilla.com.
[9]. Google Accounts. 2006. "Edit Password." https://www.google.com/accounts/EditPasswd
[10] Klein, D. V. 1990. ''Foiling the Cracker'' − A Survey of and Improvements to UNIX Password Security," Proceedings of the second USENIX Security Workshop. pp. 5 – 4.
[11] Onibere E. A. and Egwali A. O. 2006 Analyzing Factors Affecting User Password Practices: A Survey. Nigerian Journal of Computer Literacy. 7, (1) pp. 80 – 98.