Journal of Internet Banking and Commerce

An open access Internet journal (http://www.arraydev.com/commerce/jibc/)

Journal of Internet Banking and Commerce, April 2010, vol. 15, no.1
(*http://www.arraydev.com/commerce/jibc/*)

Mnemonic Passwords Practices in Corporate Sites in Nigerian

Egwali Annie Oghenerukevbe, D.M.E., B.Sc. and M.Sc.
Lecturer, Faculty of Physical Sciences, University of Benin, Benin City. Nigeria
Postal Address: **Computer Department. Faculty of Physical Sciences. University of Benin. Nigeria.**
Email: **egwali.annie@yahoo.com**
Egwali Annie Oghenerukevbe is a lecturer in Faculty of Physical Sciences. University of Benin. Benin City. Nigeria. Her area of interests includes Information Technology, Software Engineering, Gender studies, E-commerce, Electronic Marketing and Software Security. To date, she has supervised several undergraduate and postgraduate students. She is currently carrying out analysis on issues relating to developing an enhanced Authentication Model into a Paperless Office Environment. She is a member of International Network for Women Engineers and Scientists (INWES), Nigerian Computer Society (NCS) and Third World Organizations of Women Scientists (TWOWS).

Abstract

Current technological drive towards paperless mode of operations, which provides faster delivery of corporate and banking services to a wider range of customers, has resulted in the problem of identity theft which is becoming a growing problem in Nigeria. 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 an empirical investigation performed to determine the factors influencing users

mnemonic passwords practices, to analyze the strength of regular passwords and to evaluate the effectiveness of 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 customers into their sites.

Keywords: **Authentication, Mnemonic Passwords, Nigeria, Password Cracking**

INTRODUCTION

The birth of interconnectivity amongst offices and businesses has led to improved and faster delivery of services. It has also led to identity theft, which could be a fraud committed or an attempt using the identifying information of another person without lawful authority. The identifying information could be any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual. To protect sensitive information textual passwords are still the most pervasive tool used in organizations today. The popularity of the method lies in its being accepted widely by users and being easy to implement (e.g., Pinkas and Sander, 2002; Viega, 2005). Under a password system, a user accessing an electronic application is requested to enter a 'shared secret' along with their user identity. The system checks the password against information in a database to ensure its correctness and thereby 'authenticates' the user.

In computer security they are the purest form of secrets that can be kept in human memory, independently of applications and infrastructures. They can be typed quickly and discreetly on a variety of devices, and remain effective in constrained environments with basic input and no output capabilities. Passwords have become the method of choice for human authentication and mental secret safekeeping, whether locally or remotely, in an online or offline setting (FDIC, 2005).

Yet passwords have drawbacks from a usability standpoint, and these usability problems tend to translate directly into security problems. The "password problem," as formulated by Birget, et. al., (2005) and as posited by Wiedenbeck, (2005), 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 is impossible for humans, for studies on password selection, memorability and usability conclude that people choose poor passwords (Ahmet, 2005; Birget et. al. 2006; Perrig and Song, 1999). Users tend to choose short passwords and derive them from personal information that is easily guessable. Users must also manage many passwords (Sasse, et. al., 2001; Brown, et.

al., 2004) and often reuse a password across different accounts (Dhamija and Perrig, 2000). Password problems are very difficult to manage, a single local computer network with hundreds or thousands of password-protected accounts only needs one to be compromised to give an attacker entree to the local system or network. A skillful intruder may break into one system and never harm it, using it instead as a platform for attacks on a population of millions of targets. This reality is exacerbated by the increasing ability of systems to mount offline and online attacks.

These drawbacks are in reality having an enormous impact in the adoption of paperless office environments in Nigeria. Internet banking, which is one form of such a paperless environment is slowly been embraced by customers because Internet practice in Nigeria has been abused by cyber attackers who use real and deceptive websites to scoop user's sensitive information and password identities (Ezeoha, 2005; Egwali, 2008). It is believed that if customers make use of mnemonic passwords, which contains seven to nine letters from the different character sets and is made of up of meaningful words, users will be able to develop high entropy passwords that will minimize or counter identity attacks.

Unfortunately mnemonic passwords do not remove the possibility of vulnerabilities like social engineering, theft and dictionary attacks. Kuo et al. (2006) collected survey data comparing mnemonic passwords against regular passwords from 290 respondents and discovered that most of the mnemonic passwords were based on external sources, such as famous movie quotes or song lyrics. This makes the mnemonic passwords have the potential to be even more vulnerable than regular passwords since it would be trivial for attackers to build an attack dictionary based on such external sources. It was also concluded that there is little empirical data on the quality of mnemonic passwords that users select in practice. For it is not very clear whether mnemonic passwords are as strong as commonly believed. There is therefore need for more indebt knowledge of user mnemonic password practices and to ascertain if it provides the complete solution to the password problem.

This paper describes an empirical investigation performed to determine the factors influencing users mnemonic passwords practices, to analyze the strength of regular passwords using the password algorithm (Mac OS X, 2006; Mozilla Corporation, 2006; Google Accounts, 2006) and to evaluate the effectiveness of mnemonic passwords using a generated dictionary that incorporates common and local expressions within the Nigerian context.

REVIEW OF LITERATURE

Several studies on user passwords have been conducted to determine the strength of users mnemonic passwords against attacks. Yan et. al., (2004) conducted a study with 400 students, and evaluated the security and memorability of "regular" passwords, mnemonic passwords and random passwords. They 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, (2005) collected 1,200 employees passwords in the United Kingdom and concluded that people select passwords that represent themselves. Bunnell et. al.

(1997) focused on users recall and guessing rates of text passwords. From a password survey, Adams and Sasse, 1999 concluded that users lack motivation and do not have an understanding of password policies. Weirich and Sasse (2001) 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 to password practices. More generally, studies on password selection, memorability and usability conclude that people choose poor passwords (Ahmet, 2005; Birget et. al. 2006; Perrig and Song, 1999).

Jeyaraman and Topkara (2005) developed a system that would generate a fictitious news headline as a mnemonic phrase to assist users in remembering their password. Unfortunately, the system was only tested with randomly generated lowercase passwords, for which it managed to create mnemonic headlines for 80.5% and 62.7% of six- and seven-character passwords respectively. The usability, user acceptance and memorability of such a system were not evaluated, although it is evident that those users will have more difficulties memoralizing passwords generated by the system.

RESEARCH METHODOLOGY

The aim of the study is three-fold: to determine the factors influencing users mnemonic passwords practices, to analyze the strength of regular passwords and to evaluate the effectiveness of mnemonic passwords.

Sample Selection

To appraise users RPs and MPs, a survey was conducted to gather samples of RPs and MPs. The population under investigation was students from the Department of Computer Science, University of Benin. Nigeria. Some incomplete questionnaires were rejected. In answering the questions, participants were instructed to provide three RPs and three MPs but not to supply a password that they currently use or have previously used for another account for security reasons and they were assured of the confidentiality of their responses to the questionnaire. Overall 108 questionnaires were selected for the purpose of analysis (47 females, 61 males).

Instrumentation

A questionnaire was developed to collect users' personal data and samples of RPs and MPs. The questionnaire was divided into two sections: (1) demographic background, (2) samples of RPs and MPs. A copy of the questionnaire can be found in the Appendix. Demographic background included information about user's name, initials, names of friends and family members, gender, hobbies and goals. In section two, three samples each of RPs and MPs were collected making a total of 648 passwords. For RPs, users were not giving any specific guidelines so that there would not be any bias in user's choices. To produce MPs users are guided with the following directions:

i. Think of a memorable sentence or phrase containing at least four or more words that can be remembered easily.
ii. Select a letter, number, or special character to represent each word in your password. A common method is to use the first letter of every word.

iii. Ideally, the password should contain a mixture of lower case and upper case letters, numbers, punctuation, and special characters (such as ^ or %).

Data Analysis Method

RPs was also scored based on a password algorithm, for which the passwords score *S* is derived by computing the number of characters in the password *Nc* and the character complexity Ch_n, which is determined by the number of different character sets (lower-case characters (26), upper-case characters (26), numbers 0 to 9 (10) and 33 symbols (*, @, #, %, $)) incorporated into a password. The algorithm was used to compute scores for words not in dictionary, but for words found in the dictionary the score value is zero (0).

$$S = \begin{cases} Log_{10}((Ch_n)^{Nc}), & Ch_n \leq 36 \\ 0 \end{cases}$$

For MPs, the effectiveness of user's choices of MPs was evaluated by analyzing the quantitative value of users MPs when compared with the generated MPs dictionary.

To generate MPs for the dictionary, a number of techniques were employed:

(i) Each word in the expression is replaced with the character and digit that is phonetically equivalent. A sample of expressions and their mnemonic equivalent is represented in table 1.

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

(ii) Variations were introduced by replacing a particular character or digit with more than one type of word. In this case, the original expression can always be derived from the expression context if need be (see table 2).

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

(iii) Permutation was applied by interchanging upper and lower case letters (i.e. ‘‘Oluwatosin’’ would also be analyzed as ‘‘OluWaTosin” , “oluwaTosiN’’), alter some letters to numbers within the word string (i.e. Bosede would also be accessed as “B0sede” by changing alphabet “o” to number “0”) (see table 3).

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,**

(iv) 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 system 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.

Over 39055 passwords and expressions were collected including words from the King James Version bible and paired words concatenated to form expressions. Participants constructed MPs with words from expressions. 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.

RESULTS AND DISCUSSIONS

Cracking Users RPs and MPs

Table 4: Samples of Users RPs and MPs Cracked (324 RPs and 324 MPs user passwords)

Dictionary Words	Dictionary Size	Duplicated Passwords	Search Space	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**	**2.78**
Total	**39055**	**7207**	**31848**	**251**	**38.7%**

Table 4 reveals findings from passwords cracked 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 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 surveys (Klein, 1990; Yan, et. al., 2004).

Factor Determining Users RPs

Table 5: Factor Determining the Users RPs

Determining Factors						
Passwords	Personal Names	User Personal Information	Religious Background	Family Background	Life Philosophy	Goals
RPs	**93 (28.7%)**	**125 (38.6%)**	**11(3.4%)**	**15 (4.6%)**	**64 (19.8%)**	**16 (4.9%)**

Table 5 shows the determining factors influencing the RPs of users. Findings revealed

that user's passwords choices are affected mostly by the following six factors: personal names, user personal information, religious background, family background, life's philosophy and goals. Users personal information was discovered to be the most influencing of all the factors, a case in point is that of a user whose native name is "Onyeka", and yet had one of the derived RP as "onyechukwu". Not only is this password linked with the user's personal data, it is also linked with her religious background (Onibere and Egwali, 2006). Thus having a vivid idea of who a system user is most times can give a password cracker an added advantage.

Evaluation of RPs and MPs Strength

Factors	RPs	MPs
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 RPs and MPs were analyzed using the password algorithm. There was no significant difference in the RPs and MPs employed by users in terms of the password length *Nc* and the character complexity Ch_n. It was evident that creating longer and more complex passwords increases the strength of the passwords. Using one-way ANOVA, the following scores were derived $t(326) = 2.3$, $p < .005$).

PRACTICAL IMPLICATION

This survey is part of an analysis on developing an enhanced authentication model that will free users from the crisis inherent the password model. Findings from this background analysis on users RPs and MPs, confirmed the fact that to enhance computing system strength against attacks, an alternative and more robust authentication model should be developed that will completely eradicate the password problem. The major aim then is to devise authentication mechanisms for systems that are well suited to the typical interfaces and capabilities supported by offline and online systems. A model is proposed, which is called *Shield* that amalgamated multiple authentication factors. It incorporates some of the capabilities of mnemonic passwords, graphical password modes and fingerprint biometrics (future works on *Shield* will be presented in subsequent papers). This makes it significantly more difficult for an intruder to gain access. The general concept is illustrated in Figure1.

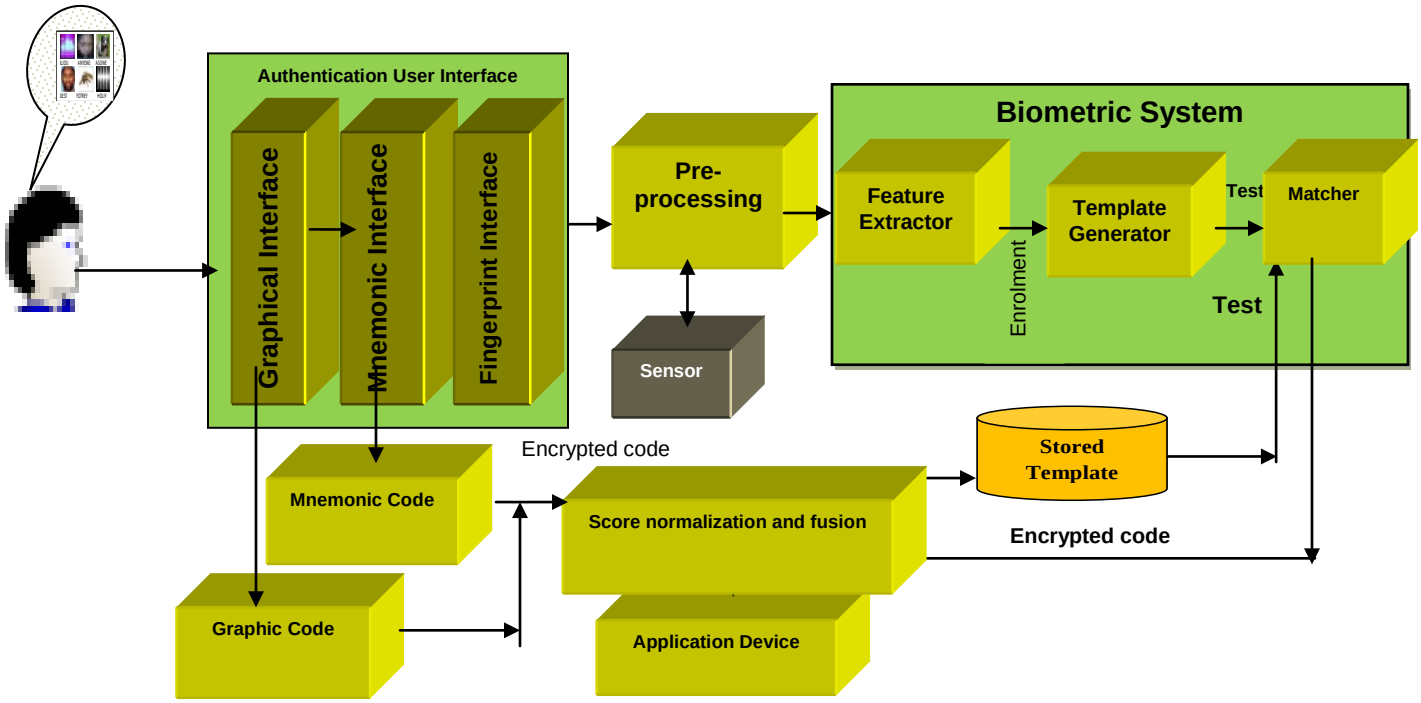

Figure 1: General Concept of *Shield:* The user clicks on a graphic displayed and its equivalent mnemonic code and then fingerprint on the sensor device, the user unique biometric feature is extracted and encrypted.

Shield interface presents the user with a full screen display of basic everyday images. The user clicks on a graphic displayed and its equivalent MP and then fingerprint on a fingerprint sensor device. The user's unique image, MP and biometric feature is extracted and encrypted. Thus by means of *Shield* most of the intricacies associated with the 'user name and password' model is completely eradicated. There are several limitations in this study, presently the study centers on the use of RPs and MPs, there is the need to investigate user perception and acceptance of other authentication models like biometrics systems and graphical passwords in the Nigeria context and security indicators in some authentication interface (Egwali, 2008). User's performance when a multifactor authentication model is employed should also be investigated. Analytical frameworks are also needed for comparing the performance of RPs, MPs, and multifactor models and a mechanism to appraise the various systems malleability to attacks. These and more issues need to be addressed in a systematic way in developing a foolproof authentication model for a wide-scale deployment.

CONCLUSION

This study discloses some major factors motivating user RPs and MPs selections, it also make known the susceptibility of present MPs to attacks, the ethnicity that stimulate these user practices. 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, due to the fact that the space of possible expressions is virtually infinite.

Findings reveal that majority of survey respondents based their RPs on five factors: personal identification information, names relating to religious background, names of some member of family, values and thinking of user and personal goals. Thus although users' context allows the deployment of MP strategies for password memorization and MPs are more resistant to brute force attacks, as time progresses MPs could become more vulnerable to attacks. Therefore it should not be regarded as the absolute solution for the password dilemma. For MPs does not remove the possibility of vulnerability like social engineering, theft and identity attacks.

RECOMMENDATION

1. Shielded authentication operation that is not vulnerable to identity attack should be employed in all sites in Nigeria. In particular, fingerprint authentication merged with mnemonics and customized graphical models that employs the `challenge response` and one-time user authentication mechanisms would be effective against offline and online identity attacks.
2. Authentication models can be designed and analyzed separately from any particular modalities used in implementation. Thus a framework can be designed that enable users select modalities suitable to their particular circumstances. And because there is security and usability implications that vary with the modalities and these will also have to be studied and developed in such a way that efficiency is not compromised.
3. In sites where a customer's negligent authentication behavior can put others at risk, it may be practical to leave users to their own authentication devices or to enable the capture of a single authentication identity ineffective for replay attack.

REFERENCE

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

Ahmet E. D., Nasir M. and Birget J. (2005). Modeling user choice in the PassPoints graphical password scheme. *Proc. Human-Computer Interaction International*, in press.

Birget J.C., Hong D. and Memon N. (2006). Graphical passwords based on robust discretization", *IEEE Transactions on Information Forensics and Security* 1(3) 395-399. (Earlier version: Cryptology ePrint Archive, http://eprint.iacr.org/2003/168.

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

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

Dhamija R. and Perrig A. (2000). Dejµa vu: A user study using images for authentication. In *Proc. of the 9th USENIX Security Symposium*, 2000.

Egwali, A.O. (2008). Customers Perception of Security Indicators in Online Banking Sites in Nigeria. *Journal of Internet Bav nking and Commerce, vol. 13, no.3.*

Google Accounts. (2006). "Edit Password." https://www.google.com/accounts/EditPasswd

Klein, D. V. (1990). ''Foiling the Cracker'' A Survey of and Improvements to UNIX Password Security," *Proceedings of the USENIX Security Workshop*.

Mac OS X (2006). Password Assistant. "Passwords: Safety in Numbers." http://www.apple.com/macosx/tips/password13.html

Mozilla Corporation,(2006).http://www.mozilla.com.

Onibere E. A. and Egwali A. O. (2006). Analyzing Factors Affecting User Password Practices: A Survey*. Nigerian Journal of Computer Literacy*. Vol 6, No. 1.

Petrie H. (2005). Password clues. http://www.centralnic.com/news/research.

Perrig, A. and Song, D. (1999). Hash Visualization: A New Technique to Improve Real World Security. In *International Workshop on Cryptographic Techniques and E-Commerce.* 131–138.

Pinkas, B., Sander, T., (2002). Securing passwords against dictionary attacks. In: *Proceedings of the Ninth ACM Conference on Computer and Communications Security. ACM*, Washington, DC, pp. 161–170.

Sasse, M. A. Brosto S. and Weirich, D.(2001). Transforming the 'Weakest Link' a Human Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal*, 19(3):122{131.

Viega, J., (2005). Solutions tT Many of Our Security Problems Already Exist, So Why Are We Still So Vulnerable? *Queue,* 41–50.

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

Weirich D. and Sasse. M. A. (2001). 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. ACM Press.

Yan, J., Blackwell, A., Anderson, R., and Grant. A. (2004). Password Memorability and Security: Empirical results. *IEEE Security and Privacy*, 2(5):25{31.