Resolving the Password Security Purgatory in the Contexts of Technology, Security and Human Factors

Muhammad Adeka, Simon Shepherd, Raed Abd-Alhameed
School of Engineering, Design and Technology, University of Bradford, Bradford, West Yorkshire, BD7 1DP, United Kingdom
{M.I.Adeka@student.,S.J.Shepherd@,R.A.A.Abd@}Bradford.ac.uk

***Abstract* - Passwords are the most popular and constitute the first line of defence in computer-based security systems; despite the existence of more attack-resistant authentication schemes. In order to enhance password security, it is imperative to strike a balance between having enough rules to maintain good security and not having too many rules that would compel users to take evasive actions which would, in turn, compromise security. It is noted that the human factor is the most critical element in the security system for at least three possible reasons; it is the weakest link, the only factor that exercises initiatives, as well as the factor that transcends all the other elements of the entire system. This illustrates the significance of social engineering in security designs, and the fact that security is indeed a function of both technology and human factors; bearing in mind the fact that there can be no technical hacking in vacuum. This paper examines the current divergence among security engineers as regards the rules governing best practices in the use of passwords: should they be written down or memorized; changed frequently or remain permanent? It also attempts to elucidate the facts surrounding some of the myths associated with computer security. This paper posits that *destitution* of requisite *balance* between the *factors of technology* and *factors of humanity* is responsible for the purgatory posture of password security related problems. It is thus recommended that, in the handling of password security issues, human factors should be given priority over technological factors. The paper proposes the use of the (k, n)-Threshold Scheme, such as the Shamir's secret-sharing scheme, to enhance the security of the password repository. This presupposes an inclination towards writing down the password: after all, *Diamond, Platinum, Gold* and S*ilver* are not memorised; they are stored.**

Keywords – technology; cryptography; computer security; social engineering; human hacking; socio-cryptanalysis; password; password repository; purgatory

I INTRODUCTION

A summary of definitions indicate that a password or passphrase is a secret word/phrase, string of characters, or some form of interactive message or signal that is used for authentication; to prove identity or gain access to a resource/place[1],[2]. Thus, in a nutshell, a password is a basic method of access control; to grant or deny access and determine the extent or level of authorisation, in some cases [3]. Other means of user authentication include:[4] Smart card or other token; Fingerprint, Retinal image, {Iris & retinal identification and vein patterns [5]}; Voice and Facial pattern; Password or PIN . It is note-worthy that, despite significant advances in graphic-based approaches, password remains the most common means of authentication,[3] The word *purgatory,* in the context of this paper, denotes a miserable situation that is of critical, complex and/or unusual difficulty.[1]

From Polybius' description of the system for the distribution of watchwords in the Roman military, [25] it is obvious that passwords or watchwords have been used since ancient times. In the military tradition, the password system operates as a pair of secret words or phrases; a *challenge* and *response.* For instance, in the opening days of the Battle of Normandy, paratroopers of the US 101st Airborne Division used the password *flash*, which was presented as a challenge, and answered with the correct response, *thunder*. The challenge and response were changed every three days. Similarly, the US paratroopers used a device known as a *"cricket"* on 'D-Day' (Tuesday, 6 June 1944 by 6:30 am), in place of a password system, as a temporarily unique method of identification; one metallic click given by the device in lieu of a password challenge was to be met by two clicks in response.[2]

Passwords have been used with computers since the earliest days of computing. MIT's Compatible Time-Sharing System (CTSS), one of the first time-sharing operating systems, was introduced in 1961. It had a *login* command that requested a user password. When the user typed in a *password*, the system would turn off the printing mechanism, so that the user might type in his password with privacy [29].

As a basic method of access control, passwords constitute the first line of defence in most computer-based information security systems [6]. Studies have shown that most of the problems associated with the users' care-free attitude have a lot to do with multiplicity of passwords required of every user [5]. Experience shows that an active Internet user has over 60 passwords and PINs for various applications and services; of these, those with the best

memories might not be able to memorise up to 25% [7]. Thus, the resultant problems include storage, password length and composition. As a result, in order to relieve the brain of undue stress, password users resort to attitudes that are inimical to password security. The security risk associated with such attitudes is widespread, as a study showed that 50% of users wrote their passwords down [6]. Experts are now divided as regards whether it is better to write down the passwords or not.

A synthesis of security guidelines for password usage shows that there is no common standard for passwords; different systems have different requirements. If this situation is analysed against the backdrop of the fact that an average user has several passwords, all of which are expected to be strong, in conjunction with unavoidable human fallibility, it is obviously impracticable for any human being to observe all the conditions associated with the password system. Thus, since it is the security of the total system that is important, this paper, which is an aspect of an ongoing research work at the University of Bradford, [8] is designed to propose a possible way out in respect of the password security purgatory phenomenon, by thinking of passwords that would take both human and security factors into consideration [6].

In an effort to attain the objective declared above, this paper will cover some of the attempts at resolving the password security problem, a survey on password security awareness in developing countries, the password security problem and a proposal for a suggested solution.

II ISSUES RELATING TO PASSWORD SECURITY

A Factors in the Security of a Password System

The security of a system that is protected using passwords depends on several factors. Among these is the need for the overall system to be designed for sound security, with protection against viruses, eavesdroppers and similar threats. Physical security against threats like *shoulder surfing, video camera* and *keyboard sniffers* should also be taken care of. Passwords should also be chosen such that they are hard to guess and also hard for an attacker to discover using any of the available automatic attack schemes. It is now common practice for the computer to hide passwords as they are being typed as a measure against bystanders reading the passwords. Since this practice may lead to errors and stress, thereby encouraging users to choose weak passwords, experts are now of the view that the system should be designed such that users have the option to show or hide the passwords as they are being typed [9]. Password strength is a measure of how effective is a password in resisting guessing and brute-force attacks; it is a function of length, complexity and unpredictability [10].

B Multiplicity of Passwords and Associated Problems

The measure of carelessness associated with the use of passwords is amazing. However, studies have shown that most of the problems associated with the users' care-free attitude in respect of password usage have a lot to do with multiplicity of passwords used by an individual [5]. Experience has shown that an active Internet user could have over 60 passwords and PINs for various applications and services; of these, those with the best memories might not be able to memorise up to 25% [7]. Thus, the resultant problems include storage, password length and composition. As a result, in order to relieve the brain of undue stress, password users resort to attitudes that are inimical to the security of the passwords, and, by extension, security of the system they were designed to protect. These negative attitudes include: writing all passwords in a diary; using the same password for all applications; relating the password to the particular application, e.g., using the room number and occupant's initials as access to the office door; using very simple configurations such as 12121212, 12345678, or 1a2b3c4d; pasting passwords on the wall, board or computer, etcetera. The security risk associated with these practices is widespread, as a study showed that 50% of users wrote their passwords down [6].

C Password Repositories

The multiplicity of passwords has engendered the problem of password storage. This has given rise to many software applications designed to facilitate password management. These are collectively called *wallets* and are in two different varieties. The first is a username/password repository; an encrypted file kept in one's computer that holds information which one needs to log into one's various accounts. The most prominent of these is *Darn! Passwords*![7],[11] It has a password generator that can make up passwords for various applications and allows one to drag one's passwords into the application or Web site that one is using. It allows one to remember only one password instead of many. Similar applications are *Password Safe* [12] and *Q*Wallet*, [13] both for windows. *Selznick PassWallet* [14] provides similar functionality on the Macintosh and Palm OS. Apparently, no similar product exists for UNIX or LINUX.

D Security Guidelines on Password Usage

It is usually better to have passwords centrally controlled, if possible. Whatever the case, in order to improve the strength of access security, users are *usually* advised to follow some guidelines, which include:[5] It should be kept absolutely secret; not divulged to any other user; It should not be written down or recorded where it can be accessed by other users; It must be changed if there is the slightest indication or suspicion of a compromise; It must be changed when a member of the organisation leaves the group or changes task; It should be at least eight characters long (alpha-numeric with mixed case/symbols) [2]; It should not be formed from any obvious source - e.g. username or group/company/project name; It must be changed monthly or at least bi-monthly; It must be changed more frequently the greater the risk or more sensitive the assets being protected; It must not be included in an automated log in procedure, i.e. not stored in a macro function; It should not be a dictionary word [2].

E Guidelines for Strong Passwords

Guidelines for choosing good passwords are designed to make passwords less easily discovered by intelligent guessing. Common guidelines include:[15],[16] a minimum password length of 12 to 14 characters if permitted; generating passwords randomly where feasible; avoiding passwords based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, etcetera; including numbers and symbols in passwords if allowed by the system; if the system recognizes case as significant, using capital and lower-case letters; avoid using something that the public or workmates know you strongly like or dislike; use acronyms of mnemonic words/phrases; providing an alternative to keyboard entry (e.g., spoken passwords, or biometric passwords); requiring more than one authentication system, such as a 2-factor authentication (something you have and something you know); write down your passwords.

From the above, it is clear that experts are now divergent as regards whether it is better to write down the passwords or not. Some guidelines advise against writing passwords down, while others, noting the large number of password protected systems users must access, encourage writing down passwords as long as the written password lists are kept in a safe place, such as a wallet or safe, not attached to a monitor or in an unlocked desk drawer [16]. In addition, some even argue that the concept of password expirations is now obsolete, [17] for the following reasons: asking users to change passwords frequently encourages simple and weak passwords; if one has a truly strong password, there is little point in changing it - changing passwords which are already strong introduces risk that the new password may be less strong; a compromised password is likely to be used immediately by an attacker to install a backdoor, often via privilege escalation. Once this is accomplished, password changes won't prevent future attacker access; mathematically speaking, it doesn't gain much security at all - moving from never changing one's password to changing the password on every authenticate attempt (pass or fail attempts) only doubles the number of attempts the attacker must make on average before correctly guessing the password in a brute-force attack - one gains much more security just increasing the password length by one character than changing the password on every use.

F Guidelines on Password Management

A password management system is an administrative arrangement aimed at providing an effective interactive resource that ensures the quality of the passwords and enforces their use in tune with the security manager's policy. In general, password management should enable secure login procedures and protect passwords against unauthorised use and access [5]. This includes measures which ensure that passwords are stored in files that are separate from the main application system data, using a one-way encryption algorithm. These measures offer some protection against *password cracker* programs and dictionary attacks. As part of the separation process between the client and the producer, the initial (default) passwords from the manufacturer must be replaced after equipment installation [5].

G Training and Security Awareness Education

Every organisation should have a security awareness training policy which ensures that organizations are responsible for not only training their own personnel, but also their agents and contractors that have access to their facilities. Initial training will need to include a review of the requirements and tailored training needs to specific security policies, processes and technology of your organization, based on the level of security responsibilities for different segments of users.

A security training program should include awareness education covering the organizational security policy, password maintenance, incident reporting, and viruses; periodic security reminders conducted as updates to the basic security education; user education concerning virus protection, including identification, reporting and preventive measures; user education in importance of monitoring log-in success/failure, and how to report discrepancies,

including employee responsibility for ensuring security of information; and user education in password management, including meticulously thought out organizational rules to be followed in creating, changing and ensuring confidentiality of passwords [24]. Personnel should also be informed on the need for the various techniques employed in the organisation's password security architecture as an important means of checkmating *human hacking or social hackers (socio-cryptanalysts).* Let all and sundry be equipped with the knowledge that there can be no technical hacking in vacuum (independent of human hacking), and that countering the SE attacks is indeed a purgatory venture (very difficult, complex and complicated endeavour). This underscores the significance of building social engineering education into all aspects of human activities, especially within the security arena [27],[28].

H Eight Myths of Computer Security

Quoting Mark Twain, Ross [26] stated that: "It ain't what you don't know, it's what you know that ain't so." Just as any other industry, Information Security has its myths and misconceptions. They can be harmful if they cause unnecessary squandering of limited resources in the wrong areas, or rely on faulty ideas and techniques. Two of the eight myths which are relevant for this discussion include:

- Myth #1-Complex passwords provide the best security
- Myth #2-Mandatory password changes improve security

In response to the *Myth #1*, many organizations have long lists of rules governing the content of passwords, primarily designed to defeat brute-force attacks; this has not succeeded due to rapid advancement in computing power and failure of many organizations to adequately monitor for failed login attempts. This seems to have eroded the value of the password as a single line of defence. Other disadvantages of complex passwords include the difficulty in remembering them, costs of generation and enforcing the password rules, as well as supporting users who have forgotten their passwords. In addition, users are sceptical of a system that imposes so many rules and regulations, which they perceive as a burden. This results in evasive attitudes, with attendant consequences. There would be need for the advocates of complex passwords to take a lesson from the banking industry, where Automated Teller Machine (ATM) cards are able to use simple 4-digit numeric passwords (PINs) because ATMs will disable a particular card if an incorrect PIN is given three times in succession [26]. A computer access control system could perform a similar function. If an account registers three successive failed login attempts, the system should automatically lock out that account. To prevent denial-of-service (DoS) attacks that would lock out legitimate users, the system should automatically remove the lock-out after some period of time; not more than 15 minutes. Thus, the temporary lock-out would be of only a minor inconvenience to a forgetful user, but sufficient to make exhaustive search attacks impractical. Hence, a system of simple passwords combined with temporary lockouts would defend against brute-force attacks, while at the same time eliminating the cost and usability problems of complex passwords.

With regards to *Myth #2*, some organizations even specify minimum password ages (to prevent users from immediately switching back to the previous password); password histories to prevent re-use of passwords; and minimum number of characters to change to ensure that a new password is *different enough* from a previous one. All of these elaborate rules make authorised access difficult, while driving up administrative and support costs for implementing and enforcing the rules. The objective for mandatory password changes stems from belief that passwords do *leak out* over time; but mandatory password changes address only a symptom, not the underlying cause of the leakages. Eliminating account sharing, prompt account closing when users depart, regular auditing of all accounts, and educating users not to divulge passwords under any circumstances would be far more effective for addressing the sources of the leakages [26].

III A SURVEY ON PASSWORD SECURITY AWARENESS IN DEVELOPING COUNTRIES

Internet world statistics [18] shows a lot of increase in the number of Internet users all over the world. The last 3 global statistics are as follows: March 31, 2011 - 2,095,006,005 (Africa: 118,609,620); December 31, 2011 - 2,267,233,742 (Africa: 139,875,242); June 30, 2012 - 2,405,518,376 (Africa: 167,335,676). This statistics shows that the use of Internet by the developing world, using Africa as a case study, is not only increasing by population, but also by global percentage. Hence, [8] became interested in finding out the state of Internet security awareness by conducting a survey between February and August 2012, in an African country. The target population was the organisational executives from the level of *Senior Enterprise Officer* and above. Altogether, 66 officials of ages from about 30 upwards responded; 66 responses were used to plot Figures 1 and 2, while 26, picked at random, were used to plot Figures 3 and 4. Figures 1 and 2 covered responses from 3 organisations, while Org. 4 is the grand total of responses from all the three organisations, to reflect the national statistics. Figures 3 and 4 analyse the responses

by rank (and age; to some extent). Only three of the eleven questions in the questionnaire were used in this analysis; Questions 2, 4 and 5.

Figure 1 reflects the answers to Question 2: Do you have a password for granting or denying access to your computer? - answer *Yes* or *No*. The bar labelled Variable *2a* represents *Yes*, while the maroon-coloured bar represents *No.* Figure 2 reflects the answers to Question 4 by organisation: What is the length of your email password? – Answers: Less than eight characters; eight characters; more than eight characters; and others (please describe). Figure 3 analyses responses to Question 4, by rank, seniority or appointment: DD-Up means *from Deputy Directors upwards;* AD-Down means *from Assistant Directors downwards.* Figure 4 reflects responses to Question 5: What is the nature of your passwords? – Answers: *Meaningful/easily remembered* (MF-ER); *Meaningless/easily remembered* (ML-ER); *Meaningless/hard-to-remember* (ML-HR); Others (please describe).

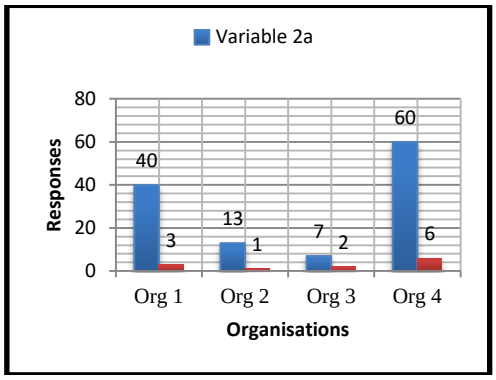

Figure 1. Level of Password Awareness

Looking at the national statistics from this survey, Figures 1 and 2 show that the levels of awareness are generally okay, but the percentage of users with passwords less than eight characters in Figure 2 is too high for comfort. Figure 4 also shows a satisfactory result with the same caveat as in Figure 2. This result also illustrates the possibility that organisational administrators from AD-Down (about the age of 40 downwards) are not only more active on the Net but also more security-conscious; the implication is that they take instructions from their less security-conscious superiors. Lastly, Figure 4 confirms the fear that most Internet users are inclined to choosing passwords that are both meaningful and easily remember-able.

IV THE PASSWORD SECURITY PROBLEM

It is the position of this paper that *destitution* of requisite *balance* between the *factors of technology* and *factors of 'humanity'*, as defined [1], is responsible for the purgatory posture of password security related problems.

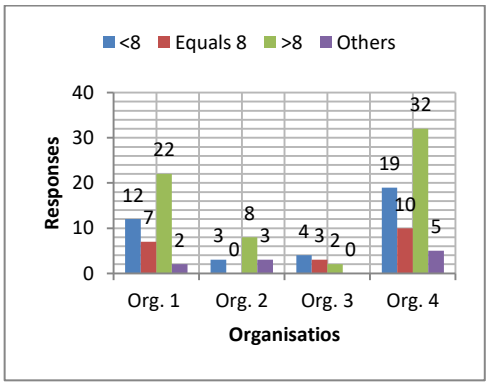

Figure 2. Significance of Password Length Awareness

This is because security countermeasures mostly focus on partial security in favour of technology, using various cryptographic encryption techniques, to the detriment of total security incorporating humanity; bearing in mind the prevalence of social engineering realities. This is contrary to the criminal cyber attack strategy which is mostly social engineering based.

Fundamentally, the need for cryptography arose in response to the requirements to secure information, whether in storage or transit. The most primary security needs it sets out to address are *confidentiality*, *integrity*, *availability*, *authenticity*, *theft* and *non-repudiation*[19] In the case of social engineering (SE), a taxonomy of user vulnerabilities include *dishonesty*, *honesty*, *vanity*, *compassion*, *gullibility*, *curiosity*, *courtesy*, *diffidence*, *apathy*, *irresponsibility*, *naivety* and *greed* [20],[21]. Thus, SE could be seen as a glorified nomenclature for what is popularly referred to as *419* in Nigeria.

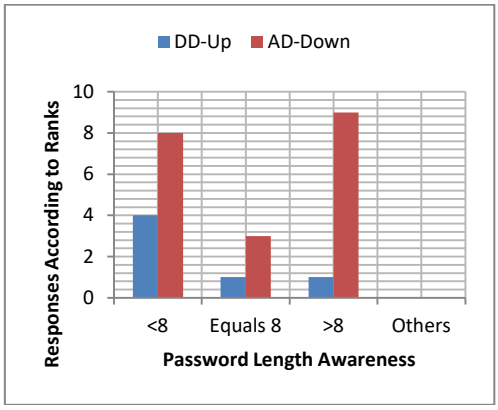

Figure 3. Significance of Password Length Awareness

Most existing security arrangements, both in theory and practice, seem to underplay the significance of the *social* aspect of cyber defence. Examples include the ITU's blue print for ensuring a global culture of cyber-security (Figure 5), which failed to assign the responsibility for the *social culture of cyber-security* to any group of professionals [22]. This under estimate of the significance of *social engineerin*g input in cyber defence is also indicative of the current UK National Cyber Security Programme (NCSP) which has allocated only *one percent* to *education* [23]; out of the £650 million ($1.01 billion) earmarked for cyber-security in the next five years (2011-2015).

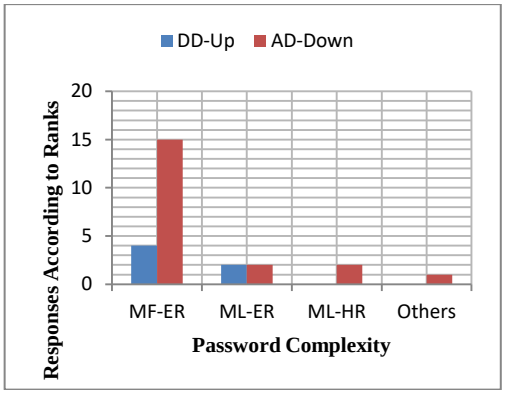

Figure 4. Significance of Password Complexity Awareness

V PROPOSAL FOR A SUGGESTED SOLUTION

In an effort to minimise the password security purgatory phenomenon, it is noted that the human factor is the most critical factor in the security system for at least three possible reasons: it is the weakest link; it is the only factor that exercises initiatives; and the factor that transcends all the other elements of the entire system. This underscores the significance of *social engineering* in every security arrangement. It is thus recommended that, in the handling of password security issues, human factors should be given priority over technological factors.

	Area of Cybersecurity Requirement	Professional Responsibility
1.	Political Culture of Cybersecurity	Legislatives, Executives, Stakeholders, …
2.	Legal Culture of Cybersecurity	Court, Judge, Prosecutor, Attorney, Regulator, Law Enforcement, …
3.	Economic & Managerial Culture of Cybersecurity	Auditors, Executive Manager, Production Manager, Human Resources Manager, CIO, CISO, ...
4.	Technical Culture of Cybersecurity	System, Network Engineer, System Administrator, Software Developer, …
5.	Social Culture of Cybersecurity	???

Figure 5. ITU Framework for a Global Culture of Cyber-security

It is realised that most of the password security-related problems have linkages with lack of secure storage system; thus encouraging users to choose weak passwords and compelling security engineers and managers to insist that passwords must not be written down and must be changed frequently. Hence, in an effort to make a contribution towards resolving this problem, this research [8] will explore the use of the (k,n)-Threshold Scheme, such as the Shamir's secret-sharing scheme, to enhance the security of password repository. This presupposes an inclination towards writing down the password: after all, *gold* and *silver* are not memorised; they are stored.

VI CONCLUSION

Experts are now divided as regards whether it is better to write down the passwords or not. Due to the large number of password-protected systems that users must access, some experts encourage writing down passwords, as long as the written password lists are kept in a safe place, such as a wallet or safe; not attached to a monitor or in an unlocked desk drawer. Similarly, some even argue that the concept of password expirations is obsolete, because mathematically speaking, the practice of changing passwords frequently does not gain much security at all; one gains much more security if one increases the password length by just one character than changing the password on every usage and attempted usage. Hence, in order to ensure password security, we must strike a delicate balance between having enough rules to maintain good security and not having too many rules that would compel users to take evasive actions which would, in turn, compromise security.

The human factor is the most critical factor in the security system for at least three possible reasons: it is the weakest link; it is the only factor that exercises initiatives; and the factor that transcends all the other elements of the entire system. This line of reasoning buttresses the significance of social engineering in security designs, and the fact that security is indeed a function of both technology and social engineering. In the course of organisational security awareness education processes, personnel should be informed on the need for the various techniques employed in the organisation's password security architecture as an important means of checkmating *human hacking or social hackers (socio-cryptanalysts).* Let all concerned know that there can be no technical hacking in vacuum (independent of human hacking).

It is realised that most of the password security related problems have linkages with lack of secure storage system; thus encouraging users to choose weak/memorable passwords, and compelling security engineers and managers to insist that passwords must not be written down and must be changed frequently. Hence, in an effort to make a contribution towards resolving this problem, this paper proposes the use of the (k, n)-Threshold Scheme, such as the Shamir's secret-sharing scheme, to enhance the security of the password repository. This presupposes an inclination towards writing down the passwords: after all, *Diamond, Platinum, Gold* and S*ilver* are not memorised; they are stored.

ACKNOWLEDGMENT

I hereby acknowledge the roles of the Petroleum Technology Development Fund (PTDF, Nigeria) for sponsoring me on the PhD Programme, and the Nigerian Army for releasing me. I am greatly indebted to my supervisors and other staffs of the School of Engineering, fellow research colleagues, especially Ogbonnaya Anoh, and the Library, ICT and other facility services at the University of Bradford, UK. Thanks to my wife, Saudat, and all my children/wards. Glorified is Allah, the Lord of His Creation.

REFERENCES

[1] Encarta Dictionary: English (UK)

[2] M. Bando, *101st Airborne: The Screaming Eagles in World War II.* Mbi Publishing Company, 2007. [Online]. Available at: http://books.google.com/books?id=cBSBtgAACAAJ. [Accessed: 20 May 2012].

[3] D.S. Jeslet et al. "Survey on Awareness and Security Issues in Password Management Strategies*." IJCSNS*, vol. 10, no.4. April, 2010.

[4] S.M. Furnell et al., "Authentication and Supervision: A Survey of User Attitudes." *Computers & Security*, vol.19 no.6, pp 529-539, 2000.

[5] R.J. Sutton, *Secure Communications: Applications and Management.* Chichester: John Wiley & Sons, Ltd. 2002.

[6] E.F. Gehringer, (2002) "Choosing Passwords: Security and Human Factors." *IEEE,* 0-7803-7824-0/02/$10.00 8.

[7] S. Farrell, "Password Policy Purgatory." *IEEE Computing Society. pp. 84-87*, 2008.

[8] M.I.U. Adeka, J.S. Shepherd, and R.A. Abd-Alhameed, "Cryptography and Computer Communications Security: *Social and Technological Aspects of Cyber Defence,"* Ongoing PhD Research Work, School of Engineering, Design and Technology, University of Bradford, Bradford (UK), (Ongoing: 2011-).

[9] Lyquix Blog: Do We Need to Hide Passwords?. Lyquix.com. [Accessed: 17 Sept. 2012].

[10] "Cyber Security Tip ST04-002". Choosing and Protecting Passwords. US CERT. [Online]. Available: http://www.us-cert.gov/cas/tips/ST04-002.html. [Accessed: 20 Jun. 2009].

[11] EmmaSoft, (2002) "Darn! Reminder Software!" [Online]. Available at: http://www.ordarn.com. [Accessed : 20 September, 20012].

[12] Password Safe 1.7.1, Counterpane Labs,. [Online]. Available: http://www.counterpane.com/passsafe.html. [Accessed: 15 Oct. 2012].

[13] Q*Wallat, http://qwallet.com. [Accessed: 15 Oct. 2012].

[14] http://www.selznick.com/products/passwordwallet. [Accessed: 15 Oct. 2012].

[15] Microsoft Corporation, "Strong passwords: How to create and use them." [Online]. Available: (http://www.microsoft.com/security/online-privacy/passwords-create.aspx). [Accessed: 11 Nov 2012].

[16] B. Schneier, 2005 "Schneier on Security: Write Down Your Password." [Online]. Availableat: (http://www.schneier.com/blog/archives/2005/06/write_down_your.html). [Accessed: 25 Sep. 2012].

[17] E. Spafford, "Security Myths and Passwords." *The Center for Education and Research in Information Assurance and Security*. 2008. [Online]. Available: http://slashdot.org/story/06/04/25/0033238/spafford-on-security-myths-and-passwords [Accessed: 21 Sep. 2012].

[18] www.internetworldstats.com. [Accessed: 15 November 2012]

[19] C. Swenson, *Modern Cryptanalysis: Techniques for Advanced Code Breaking.* Indianapolis:Wiley Publishing, Inc., 2008.

[20] J. Long, *No Tech Hacking – A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*. Syngress Publishing Inc., 2008.

[21] D. Harley, "Re-Floating the Titanic: Dealing with Social Engineering Attacks." *EICAR Conferenc*, 1998. [Online]. Available: http://cluestick.info/hoax/harley_eicar98.htm. {Accessed: 06 Oct. 2012].

[22]http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/chapter_5.html. [Accessed: 16 November, 2012].

[23] http://www.zdnet.co.uk/news/security/2010/11/17/whitehall-official-outlines-cybersecurity-funding-plan-40090898/. [Accessed: 29 Sep. 2011].

[24] http://www.nesnip.org/securitychapter1.htm#Section%20I [Accessed: 10 Oct. 2012].

[25] Polybius on the Roman Military. Available: Ancienthistory.about.com. [Online]. [Accessed: 20 May 2012].

[26] R. Oliver, *8 Myths of Computer Security*. [Online].Available: http://www.tech-mavens.com/myths.htm. [Accessed: 23 November 2012].

[27] J. Long, *No Tech Hacking – A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*. Syngress Publishing Inc., 2008.

[28] D. Harley, "Re-Floating the Titanic: Dealing with Social Engineering Attacks." *EICAR Conferenc*, 1998. [Online]. Available: http://cluestick.info/hoax/harley_eicar98.htm. {Accessed: 06 Oct. 2012].

[29] MIT Press, *CTSS Programmers Guide*, 2nd ed., MIT Press. 1965.