International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

(t, n) Threshold Scheme to Enhance the Security of the Password Repository

Malladi Venkata Naga Kiranmai[1], Avinab Marahatta[2], K. Suresh Babu[3]

[1]M.Tech. Student, School of Information Technology, JNTUH, Hyderabad, India

[2]M.Tech. Student, School of Information Technology, JNTUH, Hyderabad, India

[3]Assistant Professor, School of Information Technology, JNTUH, Hyderabad, India

Abstract: ***Passwords unit of measurement the foremost widespread and represent the first line of defense in computer-based security systems; despite the existence of further attack-resistant authentication schemes. Thus on reinforce watchword security, it's imperative to strike a balance between having enough rules to stay up good security and not having too many rules which may compel users to need evasive actions which could, in turn, compromise security. it's noted that the human issue is that the foremost vital half among the protection system for a minimum of three gettable reasons; it is the weakest link, the only real issue that exercises initiatives, furthermore as a result of the problem that transcends all the alternative components of the total system. This illustrates the importance of social engineering in security designs, {and therefore and thus and thus the indisputable fact that security is so operate of every technology and human factors; bearing in mind the actual fact that there could also be no technical hacking in vacuum. This paper examines this divergence among security engineers as regards the principles governing best practices among the employment of passwords: have to be compelled to they be written down or memorized; changed typically or keep permanent? It put together tries to elucidate the facts encompassing variety of the myths associated with computer security. This paper posits that poorness of requisite balance between the factors of technology and factors of humanity is to blame for the purgatory posture of watchword security connected problems. It's thus recommended that, among the handling of watchword security issues, human factors have to be compelled to lean priority over technological factors. The paper proposes the employment of the (k, n)-Threshold theme, just like the Shamir's secret-sharing theme, to strengthen the protection of the watch word repository. This presupposes associate degree inclination towards writing down the password: after all, Diamond, Platinum, Gold and Silver do not appear to be memorized; they are keeping.***

Keywords: Cryptography, Computer Security, Social Engineering, Human Hacking.

1. Introduction

A outline of definitions indicate that a arcanum or passphrase could be a secret word/phrase, string of characters, or some style of interactive message or signal that's used for authentication; to prove identity or gain access to a resource/place[1],[2]. Thus, in a very shell, an arcanum could be a basic methodology of access control; to grant or deny access and verify the extent or level of authorization, in some cases [3]. Different means that of user authentication include:[4] revolving credit or different token; Fingerprint, Retinal image, ; Voice and Facial pattern; arcanum or PIN . it's note-worthy that, despite vital advances in graphic-based approaches, arcanum remains the foremost common means that of authentication.[3] The word purgatory, within the context of this paper, denotes a miserable scenario that's of essential, complicated and/or uncommon issue. From Polybius' description of the system for the distribution of watchwords within the Roman military, it's obvious that passwords or watchwords are used since times of yore. Within the military tradition, the arcanum system operates as a try of secret words or phrases; a challenge and response. For example, within the gap days of the Battle of geographic region, paratroopers of the United States of America a hundred and first mobile Division used the arcanum flash, that was conferred as a challenge, and answered with the right response, thunder. The challenge and response were modified each 3 days. Similarly, the United States of America paratroopers used a tool called a "cricket" on 'D-Day' (Tuesday, half dozen June 1944 by 6:30 am), in situ of an arcanum system, as a briefly distinctive methodology of identification; one aluminous click given by the device in office of an arcanum challenge was to be met by 2 clicks in response [2]. Passwords are used with computers since the earliest days of computing. MIT's Compatible Time-Sharing System (CTSS), one among the primary time-sharing operational systems, was introduced in 1961. It had a login command that requested an user arcanum. Once the user written in a very arcanum, the system would shut down the printing mechanism, in order that the user may sort in his arcanum with privacy [29].

As a basic methodology of access management, passwords represent the primary line of defense in most computer-based data security systems [6]. Studies have shown that the majority of the issues related to the users' care-free angle have lots to try to with multiplicity of passwords needed of each user. expertise shows that a full of life web user has over sixty passwords and PINs for varied applications and services; of those, those with the simplest reminiscences won't be ready to hit the books up to twenty fifth . Thus, the resultant issues embrace storage, arcanum length and composition. As a result, so as to alleviate the brain of undue stress, arcanum users resort to attitudes that square measure hostile to arcanum security. The protection risk related to such attitudes is widespread, as a study showed that fifty of users wrote their passwords down. consultants square measure currently divided as regards whether or not it's higher to put in writing down the passwords or not.

A synthesis of security pointers for countersign usage shows that there's no common normal for passwords; completely different completely different} systems have different necessities. If this case is analyzed against the backcloth of the actual fact that a median user has many passwords, all of that square measure expected to be sturdy, in conjunction with inevitable human undependableness, it's clearly unfeasible for any soul to look at all the conditions related to the countersign system. Thus, since it's the safety of the full system that's necessary, this paper, that is a side of AN in progress analysis work the University of printer is intended to propose a doable reply in respect of the countersign security purgatory development, by thinking of passwords that may take each human and security factors into thought In a trial to achieve the target declared on top of, this paper can cowl a number of the makes an attempt at breakdown the countersign security drawback, a survey on countersign security awareness in developing countries, the countersign security drawback and a proposal for a advised resolution.

2. Background

2.1 Issues Relating to Password Security

1. 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].

2. 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 memories 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].

3. 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 Pass Wallet [14] provides similar functionality on the Macintosh and Palm OS. Apparently, no similar product exists for UNIX or LINUX.

4. 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 organization 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].

5. 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.

6. 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 unauthorized 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].

7. Training and Security Awareness Education

Every organization 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 organization'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 endeavor). This underscores the significance of building social engineering education into all aspects of human activities, especially within the security arena [27], [28].

2.2 A Survey on Password Awareness

Internet world statistics [18] shows a number of Internet users all over the world, the last 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 organizational executives from the level of Senior Enterprise officer and executives above. Altogether, 66 officials of ages from about 30 upwards responded; 66 responses were used to plot figures 1and 2, while 26, picked at random, were used to plot figures 3 and 4 Figures 1 and 2 covered responses from 3 organizations, while Org. 4 is the grand total f responses from all the three organizations to reflect the national statistics. Figures 3 and 4 analyze the responses by rank (and age; to some extent). Only three of 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 of denying the access to your computer? - Answer yes or no. the bar labeled variable 2a represents yes. Figure 2 reflects the answers to question 4 by organization: What is the length of your email password? – Answers: less than eight characters; more than characters; and others (please describe). Figure 3 analysis responses to Question 4, by rank sanitary or appointment DD-Up means from Deputy Director 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).

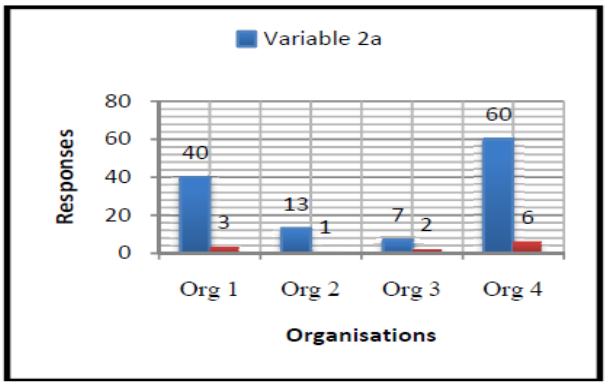

Figure 1 Level of Password Awareness

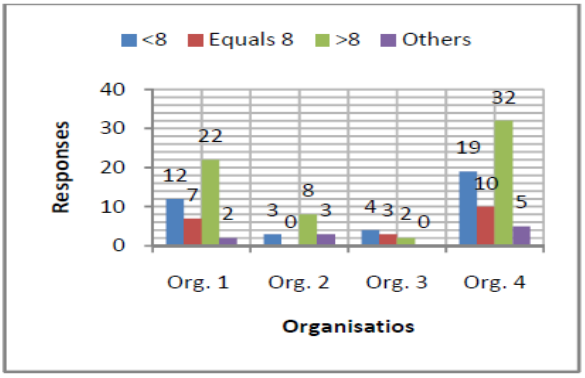

Figure 2 Significance of Password Length Awareness

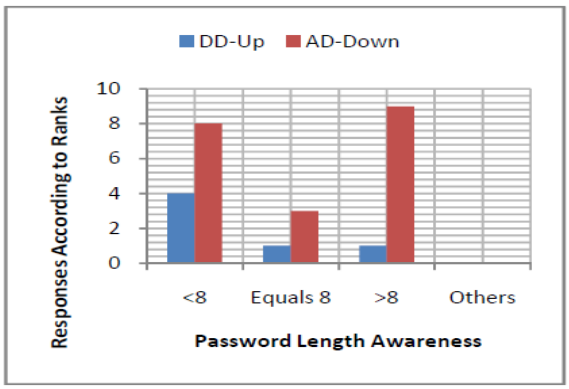

Figure 3 Significance of Password Length Awareness

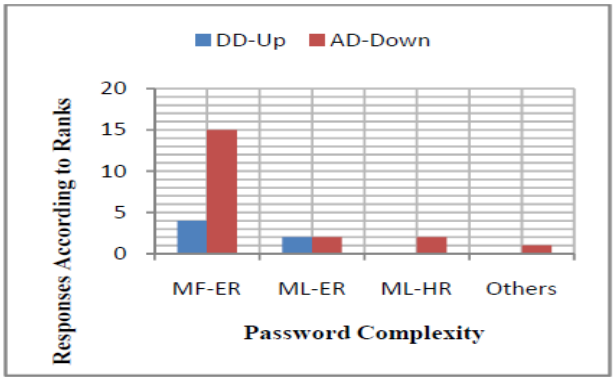

Figure 4 Significance of Password Complexity Awareness

Looking at the national statistics of this survey, Figures 1 and 2 shows 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 organizational 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.

3. Problem Statement

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 defense. 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 skeptical of a system that imposes so many rules and regulations which they perceive as a burden. This results in evasive attitude, with attendant consequences.

Some organizations even specify minimum password ages (to prevent users from immediately switching back to the previous password); password histories to prevent reuse of passwords; and minimum number of characters to change to ensure that a new password is different enough from previous password. All of these elaborate rules make authorized access difficult, while driving up administrative and support costs for implementing and enforcing the rules. The objective for mandatory password changes stems from believes that passwords do leak out over time; but mandatory password changes address only a symptom, not the underlying cause of leakages. Eliminating account sharing, prompt account closing when users leave, 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 leakages.

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, the human factors should be given priority over technological factors. It is realized 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.

4. Project Description

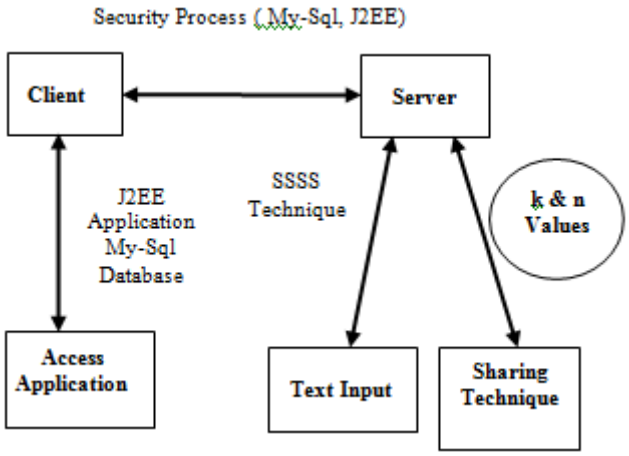

Figure 5: System Architecture

4.1 Strengthen User's Input

To strengthen the user input password we need to encrypt it and make it as unreadable formats. Make it we need some encryption algorithms. This scheme stores the inputs passwords and makes it as valuable one. To get the valuable password from the user and apply the Shamir's secret-sharing scheme to make a passwords in secure in the plain text that make the password into unreadable format, It 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.

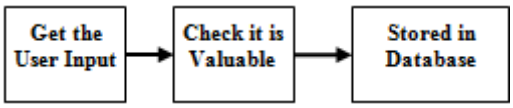

Figure 6: Strengthen User's Input

4.2 Shamir's secret-sharing scheme

Shamir's Secret Sharing is an algorithm in cryptography. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret. Counting on all participants to combine together the secret might be impractical, and therefore sometimes the threshold scheme is used where any k of the parts are sufficient to reconstruct the original secret.

Some of the useful properties of Shamir's (k, n) threshold scheme are:

1) **Secure:** Information theoretic security.
2) **Minimal:** The size of each piece does not exceed the size of the original data.
3) **Extensible:** When k is kept fixed, D_i pieces can be dynamically added or deleted without affecting the other pieces.
4) **Dynamic:** Security can be easily enhanced without changing the secret, but by changing the polynomial occasionally (keeping the same free term) and constructing new shares to the participants.
5) **Flexible:** In organizations where hierarchy is important, we can supply each participant different number of pieces according to their importance inside the organization. For instance, the president can unlock the safe alone, whereas 3 secretaries are required together to unlock it.

4.3 Encryption

In cryptography, encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text (ibid.). This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message

To encrypt the user format as to convert plain text into cipher text model. Within that we need to add polynomial algorithm and stored into the database. That wise we make our password as more secured and stored in the database.

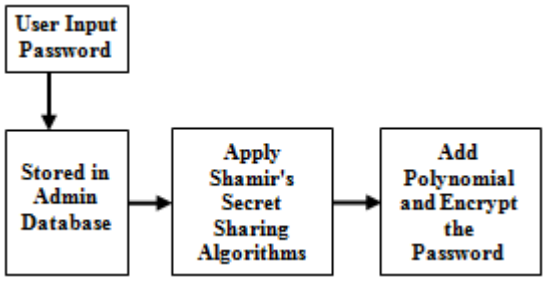

Figure 7: Encryption

4.4 Decryption

The process of decoding data that has been encrypted into a secret format. Decryption requires a secret key or password. We need to login means the passwords are decrypted from the encrypted element in the database. That retrieves the password from the polynomial conversion. It will reconstruct the cipher text and to make it as plain text.

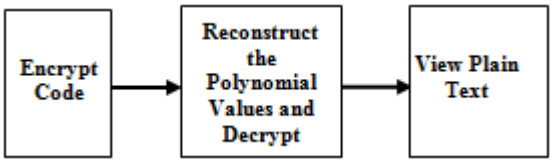

Figure 8: Decryption

4.5 Security

Security is the degree of protection to safeguard a nation, union of nations, persons or person against danger, damage, loss, and crime. Security as a form of protection is structures and processes that provide or improve security as a condition. The Institute for Security and Open Methodologies (ISECOM) in the OSSTMM 3 defines security as "a form of protection where a separation is created between the assets and the threat". This includes but is not limited to the elimination of either the asset or the threat. Security as a national condition was defined in a United Nations study (1986) so that countries can develop

and progress safely.

Security has to be compared to related concepts: safety, continuity, reliability. The key difference between security and reliability is that security must take into account the actions of people attempting to cause destruction.

Different scenarios also give rise to the context in which security is maintained:

1) With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security.
2) Measures taken by a military unit, an activity or installation to protect itself against all acts designed to, or which may, impair its effectiveness.

4.5.1 Security concepts

Certain concepts recur throughout different fields of security

- **Assurance:** Assurance is the level of guarantee that a security system will behave as expected
- **Countermeasure**: A countermeasure is a way to stop a threat from triggering a risk event
- **Defense in depth**: Never rely on one single security measure alone
- **Exploit: A** vulnerability that has been triggered by a threat - a risk of 1.0 (100%)
- **Risk:** A risk is a possible event which could cause a loss
- **Vulnerability:** A weakness in a target that can potentially be exploited by a security threat

4.6 Authentication

Authentication is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person or software program, tracing the origins of an artifact, or ensuring that a product is what its packaging and labeling claims to be.

4.6.1 Authentication methods

In art, antiques, and anthropology, a common problem is verifying that a person has the said identity, or a given artifact was produced by a certain person or was produced in a certain place or period of history.

There are three types of techniques for doing this.

1. The first type of authentication is accepting proof of identity given by a credible person who has evidence on the said identity, or on the originator and the object under assessment as the originator's artifact respectively.
2. The second type of authentication is comparing the attributes of the object itself to what is known about objects of that origin. For example, an art expert might look for similarities in the style of painting, check the location and form of a signature, or compare the object to an old photograph. An archaeologist might use carbon dating to verify the age of an artifact, do a chemical analysis of the materials used, or compare the style of construction or decoration to other artifacts of similar origin. The physics of sound and light, and comparison with a known physical environment, can be used to examine the authenticity of audio recordings, photographs, or videos. Attribute comparison may be vulnerable to forgery. In general, it relies on the facts that creating a forgery indistinguishable from a genuine artifact requires expert knowledge, that mistakes are easily made, and that the amount of effort required to do so is considerably greater than the amount of profit that can be gained from the forgery. In art and antiques, certificates are of great importance for authenticating an object of interest and value. Certificates can, however, also be forged, and the authentication of these poses a problem. For instance, the son of Han van Meegeren, the well-known art-forger, forged the work of his father and provided a certificate for its provenance as well; see the article Jacques van Meegeren. Criminal and civil penalties for fraud, forgery, and counterfeiting can reduce the incentive for falsification, depending on the risk of getting caught.
3. The third type of authentication relies on documentation or other external affirmations. For example, the rules of evidence in criminal courts often require establishing the chain of custody of evidence presented. This can be accomplished through a written evidence log, or by testimony from the police detectives and forensics staff that handled it. Some antiques are accompanied by certificates attesting to their authenticity. External records have their own problems of forgery and perjury, and are also vulnerable to being separated from the artifact and lost. Currency and other financial instruments commonly use the first type of authentication method. Bills, coins, and cheques incorporate hard-to-duplicate physical features, such as fine printing or engraving, distinctive feel, watermarks, and holographic imagery, which are easy for receivers to verify. Consumer goods such as pharmaceuticals, perfume, fashion clothing can use either type of authentication method to prevent counterfeit goods from taking advantage of a popular brand's reputation (damaging the brand owner's sales and reputation). A trademark is a legally protected marking or other identifying feature which aids consumers in the identification of genuine brand-name goods.

5. 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 organizational security awareness education processes, personnel should be informed on the need for the various techniques employed in the organization'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).

References

[1] 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].
[2] D.S. Jeslet et al. "Survey on Awareness and Security Issues in Password Management Strategies." IJCSNS, vol. 10, no.4. April, 2010.
[3] S.M. Furnell et al., "Authentication and Supervision: A Survey of User Attitudes." Computers & Security, vol.19 no.6, pp 529-539, 2000.
[4] R.J. Sutton, Secure Communications: Applications and Management. Chichester: John Wiley & Sons, Ltd. 2002.
[5] E.F. Gehringer, (2002) "Choosing Passwords: Security and Human Factors." IEEE, 0-7803-7824-0/02/$10.00 8.
[6] S. Farrell, "Password Policy Purgatory." IEEE Computing Society. pp. 84-87, 2008.
[7] 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, Schoolof Engineering, Design and Technology, University of Bradford,
[8] Lyquix Blog: Do We Need to Hide Passwords?. Lyquix.com. [Accessed: 17 Sept. 2012].
[9] "Cyber Security Tip ST04-002". Choosing and Protecting Passwords. US CERT. [Online]. Available: http://www.uscert.gov/cas/tips/ST04-002.html. [Accessed: 20 Jun. 2009].
[10] EmmaSoft, (2002) "Darn! Reminder Software!" [Online]. Available at: http://www.ordarn.com. [Accessed : 20 September, 20012].
[11] Human Factors of Security Systems: A Brief Review; Andrew Patrick, National Research Council of Canada
[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/passwordscreate.aspx) [Accessed: 11 Nov 2012].
[16] B. Schneier, 2005 "Schneier on Security: Write Down Your Password."[Online]. Availableat:
[17] (http://www.schneier.com/blog/archives/2005/06/write_ down_your. html). [Accessed: 25 Sep. 2012].
[18] 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-securitymyths-and-passwords [Accessed: 21 Sep. 2012].
[19] www.internetworldstats.com. [Accessed: 15 November 2012] International Conference on Computer Applications Technology 2013 (ICCAT'2013), January 20 – 22, Sousse, Tunisia
[20] C. Swenson, Modern Cryptanalysis: Techniques for Advanced Code Breaking. Indianapolis:Wiley Publishing, Inc., 2008.
[21] J. Long, No Tech Hacking – A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Syngress Publishing Inc., 2008.
[22] 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].
[23] http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/chapter_5.html. [Accessed: 16 November, 2012].
[24] http://www.zdnet.co.uk/news/security/2010/11/17/white hall-officialoutlines-
[25] Cybersecurity-funding-plan-40090898/. [Accessed: 29 Sep. 2011].
[26] http://www.nesnip.org/securitychapter1.htm#Section%20I [Accessed: 10 Oct. 2012].
[27] Polybius on the Roman Military. Available: Ancienthistory.about.com. [Online]. [Accessed: 20 May 2012].
[28] R. Oliver, 8 Myths of Computer Security. [Online].Available: http://www.tech-mavens.com/myths.htm. [Accessed: 23 November 2012].
[29] J. Long, No Tech Hacking – A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Syngress Publishing Inc., 2008.
[30] 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].

Author Profile

Malladi Venkata Naga Kiranmai received Bachelor of Technology in Computer Science and Engineering from Jawaharlal Nehru Technological University Hyderabad. She is pursuing Master of Technology in Computer Science in School of Information Technology, Jawaharlal Nehru Technological University Hyderabad. Her research interest is Computer Architecture, Human Computer Interaction, Wireless Network, Network Security and Data mining.

Avinab Marahatta received Bachelor of Engineering in Computer Engineering from Purbancal University. He is pursuing Master of Technology in Computer Science in School of Information Technology, Jawaharlal Nehru Technological University Hyderabad. He worked in Higher Secondary Education Board (HSEB) Nepal, under the ministry of Education as Computer Engineer. His research interests are Computer Architecture, Human Computer Interaction, Wireless Network, Network Security and Data mining.

Kare Suresh Babu has completed his Master of Technology in Computer Science from Hyderabad Central University (HCU), Hyderabad. He is the Asst. Professor and course Coordinator for School of Information Technology, Jawaharlal Nehru Technological University Hyderabad. His subjects of interests are Computer Networks, Network Security, Operating Systems, Wireless Networks, mobile Computing, Ethical Hacking and Wireless & Web Security.