"REVIEW ON SECURITY AND AUTHENTICATION SYSTEM IN ACCESSING DATA"

MITALI LAKADE[1], RUCHI KELA[2], ASHWINI[3], AMITKUMAR MANEKAR[4]
[1,2,3,4]Shri Sant Gajanan Maharaj college of Engineering,
Amravati University
[1]mitalilakade286@gmail.com
[2]ruchi.kela1995@gmail.com
[3]ashwinigugle@email.com
[4]asmanekar24@gmail.com

ABSTRACT: *Various Password authentications methods are available now a days Now a day's various complex and light weighted methods are available in various online application and E Commerce sites. Some methods are based on encryption which provide real time security and basically it's a lasts alternative. Some methods are based on biometric data where humans eye and figure prints are the key values. In this work we are trying to take a tour and collect information about all authentication methods available in today's context. While collecting information their pros and cons are measured and analysis. Finally a conclusion is drawn on the basis of these methods. A future scope is canvassed and a conclusion drawn on the basis of some parameters which will help to decide the best method for online transactions system.*

Keywords: Authentication, Security, Online Data Accessing.

1. INTRODUCTION

Spyware is a most dangerous malware that get installed on any computer without the authority or permission of the owner in order to collect the information of owner. The owner's information can be private or public, it collects information such personal details, credit card no. , password saves in chrome cookies etc. which is personal to the owner. Spyware also collect information such as user keystrokes, internet activities, sometimes slow down our computer or crash and also take space etc. So it is becoming serious issue of spyware which need to be handling in some cases, so we have many different software tools to protect this issue. Our review says there are until now so many methods for password security. The most widely used is textual password technique. Textual password is the combination of alphabet (A-Z, a-z), Digits (0-9) and special symbol (eg: @,*,-). This type of password also called as alphanumeric password. But with this many different security issues arises. The alternative to this textual password there is another technique Graphical password. To reduce all this problem of traditional methods, textual graphical password scheme using color combinations have been developed for the possible 9 alternative solution to old one traditional system. The textual password authentication is not secure and has high failure rate compare to the others because shoulder surfing is too much easy for textual based password. To overcome these, the primary design without any extra complexity into the authentication process is improved.

2. RELATED WORK

Various types of techniques are available for authentication alphanumeric password is a traditional technique which is widely used. It consists of secret series of characters. The user id and password act as user identification and authentication to access required resources. This alphanumeric password technique secures resources but it has many disadvantages. User can pick password which can be guessed easily and vulnerable to shoulder surfing. If user selects a password which is difficult to guess, then it is hard for user to remember it. Also user can become the victim of dictionary attack, brute force attack and spyware etc. Password are system generated and are difficult to remember [1]. Some researchers developed authentication methods that use Graphical Password that can overcome the problems related to traditional text password method [2]. These Graphical passwords are more difficult to break using the traditional attack methods such as brute force search, dictionary attack [3], or spyware.

Problems with textual characters:

Textual passwords [4] are the most popular user authentication method but have security and usability problems. The common human tendencies to create memorable passwords which should be small not so lengthy, as strong system assigned passwords are difficult to remember. They use to provide the same password for different accounts. Large number of passwords increases interference lead to confusion.

Some of the textual based password techniques are:

a) Encryption: - Encryption **o**f data [5] has become an important way to protect data resources especially on the internet. Encryption is the process of applying special algorithms and keys to transform data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code [6].

b) Cryptography: - Cryptography is the major element which is used to secure data or information while sharing confidential data.

There are many techniques available to secure data but still improvements and establishment of new techniques is required. In which plain text message get converted into cipher text also known as human unreadable form [8] [9] [10] [11] [12] [13].

c) One-Time Password (OTP):-Xuguang Ren, Xin-Wen Wu proposed generation of dynamic OTP.A **one-time password** (OTP) is a password which is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with text (static) passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. They have considered user's password, the authenticating time, as well as a unique property that the user possesses at the moment of authentication (for example, the MAC address of the machine that the user uses for authentication) to generate OTP [14]. This system effectively protects user's account against various attacks such as phishing attack, reply attack, and perfect-man-in-the-middle attack [15].

d) Two One-Way Hash Functions: -Huiyi L. and Yuegong Z proposed scheme which uses two one-way hash functions, one is a hash chain and another is to secure the hash chain. Hash chain is the core of the authentication scheme, and the other is use for information transmission between the user and server. This scheme presents higher security and lower computational cost [16] as well as functions of bidirectional identity authentication.

e) Two Factor Face Authentication Scheme: - Jeonil Kang, et.al in this paper, a user password is suggested [17] and a two factor face authentication scheme using matrix transformations.

f) Cryptography: - SALT (cryptography) In Cryptography, a salt is random data or string that is used as additional input to a function that hashes a password [18]. Salt is use to protect against dictionary attacks and rainbow table attacks. Randomly generated String that is the generated salt and User's password are concatenated and processed with the Cryptographic hash function and result is stored with salt in a Database.

Random function Salt is gets generated by using original password. After this generated Salt is appended to the original user's password. Then this Salt appended password is passes to Hash function which is use to generate Salt Hash password. Finally both the generated Salt Hash Password and Salt is stored in database. In this iteration count is used which is refers to the number of time that the hash function with which we are digesting is applied to its own this means that, once we generate a salt concatenated with the password then apply the hash function, get the result and again pass that result as a input to the same hash function .This process is repeated again and again a number of times. The minimum number of iteration is 1000 for more security.

g) PBKDF2 (Password Encryption):- Pseudorandom function such as cryptographic hash, cipher is applied by PBKDF2 to the user password along with salt value. This process repeated multiple times to produce derived key. This key is used as cryptographic key in subsequent operations. So PBKDF2 algorithm takes a salt, Random function which gives random value, original user's **Graphical based:**

password. Then this algorithm using number of iterations again and again Derived Key is generated which is final output. Derived key that conations salt, some random values and original password. This is for the login passkey which is makes cracking or hacking of password is quite slow and makes password more secure and protected.

h) Session Password using grid

Pair based authentication scheme

Grid: - 8x8matrixes is used to represent alphabets, digits and special symbols to the user so user has to select session password by using grid where I is row element and J is column elements. E.g. Length of the password is 8 and password is ABCDEQRS. Now we will make pairs as AB CD EQ RS .so the session password length is 4. We will select row containing character A and column containing character B. And intersection of that row and column is inserted into the password field likewise all the pairs are selected into the grid and password is entered. This new password is valid only for that session and is stored in the user log on server. The session password and 8x8 grids are sent to the server. On the server side this session password is cross checked with the user's original password. [18]

3. Biometric based authentication Techniques:

Biometric based authentication techniques, such as fingerprints, iris scan, facial recognition and other more known or futuristic biometrics [19] [20] such as gait and smell, are not adapted to the full extent. The major draw back of Biometric based approach is that such a system is costly and the identification process can be slow and often undependable [21]. [22].Jakobsson M., et.al introduced the notion of implicit authentication that consists in authenticating users based on behavioral patterns [23].

Token based authentication techniques:

A security token is a physical device that can be easily carried. A security token can be a bankcard, a smartcard containing passwords, PIN to protect a lost or stolen token. The drawback of a metal key is that, if it gets lost, it enables its finder to enter the house. There is a distinct advantage of a physical object used as an authenticator, because if it is lost, the owner can have proof of this and can act accordingly [24].

Multiple password interference in text:

The problems relating to the utility and security of multiple passwords are not largely evaluated. However, we know that people generally have difficulty in remembering multiple passwords. Since users reuse the same password for different systems as they try to login [25] hence this reduces security.

So alternative to textual password, a technique proposed is graphical password [26].In this technique the images or

shapes are used because people can remember images easily than text , it is easy for human beings to remember the places they visit, things they have seen and faces of different people. In addition, if images used in graphical password technique are large enough, the password space of a graphical password technique may exceed as compare to text-based password and thus can offer resistance to all possible attacks of text-based password. In such way graphical passwords are difficult to guess and easy to remember.

Graphical password techniques are categorized as follows:

1**) Recognition Based System:-** In this system, for registration the user has to select the certain number of images from a set of random images in an order as a password, and for authentication the user has to identify (recognize) those images in a same order.

There are some special techniques under this system:

i) Dhamija and Perrig [27] proposed a graphical authentication scheme where the user has to identify the pre-defined images to prove user's authenticity. In this system, the user selects a certain number of images from a set of random pictures during registration. Later, during login the user has to identify the pre selected images for authentication from a set of images. This system is vulnerable to shoulder-surfing.

ii) Passface [28] is a technique where the user sees a grid of nine faces and selects one face previously chosen by the user. Here, the user chooses four images of human faces as their password and the users have to select their pass image from eight other decoy images. Since there are four user selected images it is done for four times.

iii) Wiedenback et al [29] describes a graphical password entry scheme using convex hull method towards Shoulder Surfing attacks. A user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects. In order to make the password hard to guess large number of objects can be used but it will make the display very crowded and the objects almost indistinguishable, but using fewer objects may lead to a smaller password space, since the resulting convex hull can be large.

iv) Blonder [30] designed a graphical password scheme where the user must click on the approximate areas of pre-defined locations.

v) Passlogix [31] [32] extended this scheme by allowing the user to click on various items in correct sequence to prove their authenticity.

2) Recall-Based System.

In this system a user is asked to reproduce something that he created or selected earlier during the registration stage. There are some techniques under this system:

i) Jermyn, et al. [33] proposed a new technique called "Draw- a-Secret" (DAS), where the user is required to re-draw the pre-defined picture on a 2D grid. If the drawing touches the same grids in the same sequence, then the user is authenticated. This authentication scheme is vulnerable to shoulder surfing.

ii) Haichang et al [34] proposed a new shoulder-surfing resistant scheme, where the user is required to draw a curve across their password images orderly rather than clicking on them directly. This graphical scheme combines DAS and Story schemes to provide authenticity to the user.

iii) Syukri [35] developed a technique where authentication is done by drawing user signature using a mouse. This technique included two stages, registration and verification. At the time of registration stage the user draws his signature with a mouse, after that the system extracts the signature area. In the verification stage it takes the user signature as input and does the normalization and then extracts the parameters of the signature. The disadvantage of this technique is the forgery of signatures. Drawing with mouse is not familiar to many people; it is difficult to draw the signature in the same perimeters at the time of registration.

iv) In this passpoint system through complex, one can make more password .To get access user has to click close to the selected click point within specific distance i.e. 0.25 to 0.50 cm from the users click point .Sometimes it may happens that user unable to identify the exact pixel of the click point so flexibility is not there therefore we define specific area around the click point. If user can click within that range it gets access.

v) Cued click point: Cued click point [37] [38] is an alternative to pass point .In this technique we are clicking on one point on each images rather than on multiple points on single images. If user make mistake while clicking latest click point at that stage user can cancel their attempt and retry from the beginning.

vi) Soon-Nyean Cheong, et.al presented a secure two-factor authentication NFC smartphone access control system using digital key and the proposed Encrypted Steganography Graphical Password [39].

4. CONCLUSION

Various password techniques such as textual password, graphical password, behavioural and combination of graphical with textual is discuss with its pros and cons. The best alternative for textual password is a graphical password. The graphical password can reduce the burden of human memory as humans tend to remember graphics and images better. Overall it is more difficult to break graphical passwords using various attacks like brute force attack, dictionary attack, social engineering etc. We have tried our best to change the phrase that "small password is not secure and easy to guess" into "small password is secure and hard to guess" But graphical passwords are vulnerable to shoulder surfing and spyware attack. So the best alternative to such techniques is combination or

graphical with textual which constitute (colour code, grid, ciphering).In such technique we are proving small password easy to remember and secure password authentication.

5. FUTURE SCOPES

Future scope of this technique is that, as it provides more security than the others existed systems more secure login for users is possible. So this technique is not just limited for PDA i.e. personal digital Assistant but also it is very useful for providing protection against Hacking, Dictionary attacks etc. In future it will be used for Banking Applications, Military security purpose, Scientists research security, Mobile phones applications where the security is more important.

6. REFERENCES

[1] S. Wiedenbeck, j. Waters, j. C. Birget, a. Brodskiy, and n. Memon, "passpoint: design and longitudinal Evaluation of a graphical password scheme," international journal of human studies 63 (2005) 102-127.

[2] S. Wiedenbeck, j. Waters, j. C. Birget, a. Brodskiy, and n. Memon, "authentication using graphical passwords: Basic results," in human-computer interaction international (hcii 2005). Las vegas, nv, 2005

[3] P.C. van oorschot, a. Salehi-abari, j. Thorpe. Purely automated attacks on passpoints-style graphical Passwords.ieee trans. Info. Forensics & security, 5(3):393–405, 2010.

[4] S. Chiasson, a. Forget, e. Stobert, p. Van oorschot, and r. Biddle, "multiple password interference in text and click-based graphical passwords," proc. Acm conf. Computer and comm. Security (ccs), nov. 2009.

[5] Partial face recognition: alignment- free approach, shengcai liao, anil k. Jain, fellow, ieee and stan z. Li, fellow, ieee, 2011.

[6] K . Pi et al. (ijaer) 2014, vol. No. 8, issue no. Iii, Sep ISSN: 2231-5152

[7] International journal of information & computation technology. ISSN 0974-2239 volume 4, number 13 (2014), pp. 1305-1314
© International research publications house
Http://www. Irphouse.com

[8] Gary c. Kessler, "an overview of cryptography", Http://www.garykessler.net/library/crypto.html, 2014
[9]https://encryptedtbn3.Gstatic.com/images?q=tbn:and9gcr12qomdzbjetouvqfwyigk3w_M2vvcrby7wgmp77uqaic3arpmq

[10] Salah alabady, "design and implementation of a network security
5019, pp. 16–35, 2008.
Model for cooperative network", 2009

[11] Sumedha kaushik and ankur singhal, "network security using
Cryptographic techniques", 2012

[12] Vishwa gupta, gajendra singh and ravindra gupta, "advance
Cryptography algorithm for improving data security",2012

[13] University of alabama at birmingham, "ease and security of
Password protections improved", 2014

[14] International journal of network security & its applications (ijnsa), vol.4, no.2, march 2012

[15] Xuguang ren, xin-wen wu, ―a novel dynamic user authentication scheme‖, international symposium on communications
And information technologies, pp. 713-717, 2012.

[16] Huiyi l., yuegong z., ―an improved one-time password authentication scheme‖, proceedings of icct, pp 1-5, 2013.

[17] Kang, j., nyang, d., lee, k., ―two-factor face authentication using matrix permutation transformation and a user password‖,
Information science. 269, pp. 1–20, 2014.

[18] Multidisciplinary journal of research in engineering and technology volume 1, issue 2, pg.175-182

[19] M. Mosam et. Al International journal of network security & its applications (ijnsa), vol.3, no.3

[20] Xiongwu xia, lawrence o'gorman innovations in fingerprint capture devices, veridicom inc. 31 scotto pl, dayton, nj 08810, usa received21 December 2001.

[21] S. Pankanti, r. M. Bolle, a. Jain, biometrics: the future of identification, special issue of computer, vol. 33, no. 2, Feb. 2000.

[22] l. O'Gorman, comparing passwords, tokens, and biometrics for user authentication, proc. Ieee, vol. 91, no. 12, pp. 2019-2020, dec. 2003.

[23] Wayman, j., Jain, a. K., maltoni, d., &maio, d. (Eds.). (2004). Biometric systems: technology, design and performance
Evaluation. New York: springer.

[24] Huigi catuogno, clemente galdi, ‖a graphical pin authentication mechanism with applications to smart cards and low-cost Devices‖, information security theory and practices. Smart devices, convergence and next generation networks, lncs, vol.

[25] Sonia chiasson1, alain forget1, Elizabeth stobert2, p.c. van oorschot1, Robert biddle1 1school of computer

science, multiple password interference in text passwords and click-based graphical passwords, department of psychology Carleton university, Ottawa, Canada, November 2009.

[26] A. Adams, m. A. Sasse, and p. Lunt. "Making passwords secure and usable". In hci 97: proceedings of hci on people and computers, pp.1-19, London, UK, 1997. Springer-verlag.

[27] R. Dhamija, and a. Perrig. "déjà vu: a user study using images for authentication". In 9th usenix security symposium, 2000.

[28] Real user corporation: passfaces. Www.passfaces.com

[29] S. Wiedenbeck, j. Waters, j.c. birget, a. Brodskiy, n. Memon, "design and longitudinal evaluation of a graphical password system". International j. Of human-computer studies 63 (2005) 102-127.

[30] G. E. Blonder, "graphical passwords," in lucent technologies, inc., murray hill, nj, u. S. Patent, ed. United states, 1996.

[31] Passlogix, site http://www.passlogix.com.

[32] Forget, s. Chiasson, p. Van oorschot, and r. Biddle, "improving text passwords through persuasion," proc. Fourth symp. Usable privacy and security (soups), July 2008

[33] Jermyn, I., mayer a., monrose, f., reiter, m., and Rubin. "the design and analysis of graphical passwords" in proceedings of usenix security symposium, august 1999.

[34] Haichanggao, zhongjie ren, xiuling chang, xiyang liu uwe aickelin, "a new graphical password scheme resistant to shoulder-surfing

[35] F. Syukri, e. Okamoto, and m. Mambo, "a user identification system using signature written with mouse," in third Australasian conference on information security and privacy (acisp): springerverlag lecture notes in computer science (1438), 1998, pp. 403-441.

[36] X.s. Zhou and T.S. huang, ― relevance feedback
For image retrieval: a comprehensive review, multimedia systems, vol.8, no. 6 apr. 2003.

[37] S. Chiasson, p. Van oorschot, and r. Biddle, "graphical password authentication using cued click points," proc. European symp. Re-search in computer security (esorics), pp. 359-374, sept. 2007

[38]. Thorpe, j. And van oorschot, p.c. human-seeded attacks and exploiting hot-spots in graphical passwords. Usenix security symp. 2007

[39] Cheong, soon-nyean, huo-chong ling, pei-lee the, ―secure encrypted steganography graphical password scheme for near Field communication smartphone access control system, expert systems with applications 41.7, pp. 3561-3568, 2014.

7. AUTHOR PROFILE

	Mitali Lakade Perceiving the 3rd year B.E. in Information And Technology at Shri Sant Gajanan Maharaj College of Engineering, Shegaon, Dist Bhuldhan, Maharashtra , India
	Ruchi Kela Perceiving the 3rd year B.E. in Information And Technology at Shri Sant Gajanan Maharaj College of Engineering, Shegaon, Dist Bhuldhan, Maharashtra , India
	Ashwini Perceiving the 3rd year B.E. in Information And Technology at Shri Sant Gajanan Maharaj College of Engineering, Shegaon, Dist Bhuldhan, Maharashtra , India
	Amitkumar S Manekar working as assistant Professor in IT Department SSGMCE, Shegaon. His research area is Big Data analysis and High performance Computing. He has guided many Under Graduate and Post Graduate Students