I. J. Computer Network and Information Security, 2015, 3, 57-64
Published Online February 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2015.03.08

Secure Usable Authentication Using Strong Pass text Passwords

C. Shoba Bindu
Department of CSE, JNTUA College of Engineering, Ananthapuramu, Andhra Pradesh, India
Email: shobabindhu.cse@jntua.ac.in

***Abstract*—**Traditional alphanumeric passwords used for remote user authentication does not offer both usability and security. Graphical passwords were proposed as an alternative to these textual passwords for improving usability and security. This paper proposes a remote user authentication scheme, which extends the existing pass text scheme. The usability and security of the proposed scheme is analyzed. Using Morea tool the Usability of the proposed scheme is investigated.

***Index Terms*—**Authentication, Graphical passwords, Pass Text passwords, Usability.

I. Introduction

As computer security plays a vital role in our everyday life, it is important to authenticate users to different systems in order to prevent unauthorized access. In general, the alphanumerical passwords and PINs are used for remote user authentication to access the remote services. These textual passwords can be either

1. Strong passwords: Hard to remember
2. Weak passwords: Easy to remember

Users tend to choose weak passwords, which can be remembered easily and easy to use for authentication. But these passwords are vulnerable to guessing, dictionary and brute-force search attacks. In order to improve the security of these passwords, users are instructed to use strong passwords which are hard to remember and hard to crack them with automated tools.

Alphanumerical passwords are vulnerable to various attacks. To overcome the disadvantages of classical or alpha-numerical passwords, there exists a wealth of different authentication mechanisms [1] [2] [3] [4] [5]. This section gives the quick overview of these authentication techniques. According to Renaud [6] et.al, these techniques are classified into 3 types based on the following characteristics of the user:

i. Location of the user
ii. Owning of the user
iii. User's Knowledge

i. Location of the user

Location of the user is the mechanism to find the location of the user at an instant. GeoBio indicator and phone call verification are the techniques to identify the location of the user. But these two techniques are used to get the geographic location of the user but not the user.

ii. Owning of the user

This is a biometric approach in which user is authenticated by using bio-password and pass thoughts mechanisms. The Bio-password is nothing but user's iris scan, face, voice, tokens like smartcards and fingerprints can be taken as password for this classification. Pass thoughts technique is proposed by Thrope et.al [7], in which user is authenticated through the behavior of the user. User is rejected to access the system resources when he shows suspected behavior. These two mechanisms require special hardware and very expensive to install and maintain.

iii. Knowledge of the user

This mechanism is further divided into textual and graphical password system.

Textual passwords:

Textual password approach is again divided into three types which are,

- Syntactic
- Semantic
- One-time passwords

The examples of the syntactic passwords are passphrases and classical passwords. In this scheme, user needs to memorize a sequence of words or characters. The sequence is either user selected or generated for the user. User can't memorize the multiple passwords or complicated passwords for long time. If user choose easy to remember passwords then it is easy to hack with dictionary attack. So this technique provides low level of security. Check-Off-Password System (COPS) [8] is another mechanism in which user has to enter characters in any order and it is easy to remember in many different ways.

Semantic passwords also known as cognitive passwords require a user to answer the question and this answer is the key to the authentication mechanism. Renaud [6] believes in the user clarifying questions and if the answer matches with the one expected by the system then he or she is authenticated. Fact based or opinion based mechanisms are another two techniques which

provides authentication but these are not user friendly and are time-consuming.

One-time password is a password that is valid for only one login. If a hacker comes to know this code he can't reuse this for authentication. But this works only for the crucial systems where the access to the system is not necessary at all the time.

Text passwords are the most widely used passwords among several methods for user authentication, as they are simple and inexpensive to implement, need not have to carry physical tokens and hence easy to port. The single factor authentication techniques i.e. based on only passwords have their limitations such as they can be guessed, shared or lost.

The logical alternative is two factor authentication techniques, in which two methods are applied, a combination of knowledge and possession. In [9][10][11] two factor remote user authentication techniques using passwords and smartcards were proposed. [12] provides a complete solution to the online security by combining biometric templates and passwords.

The techniques using textual passwords have the drawback that the user has to memorize a hard-to-remember textual password. Graphical passwords were found to be the better alternative.

Graphical passwords:

Graphical passwords [13] are preferred over traditional passwords, because user can remember easily pictures or images than textual information. The graphical passwords are of two types: recognition based and recall based passwords.

In recognition based passwords, a user selects a series of images among many during enrollment phase and he must identify the same images in the same series during authentication phase and this leads to successful authentication.

Passfaces [14] are the most widely used recognition based passwords till now. In this scheme, users will be selecting a set of human faces at the time of registration and during the login phase the user has to select the face belonging to his password set from the panel of candidate faces. It is repeated for several rounds, and the user will be successful in logging only after executing each round successfully.

Davis et. al. [15], in their study on the pass face graphical passwords established obvious patterns among these passwords. They have observed that many of the people faces, users choose are from the same race. They identified that female faces and good looking were favored by both male and female users (Figure 1). These make the pass face password pretty predictable. This problem can be reduced by assigning random faces to users for choosing their passwords, but people feel difficult to remember the password. This passfaces [14] scheme is not resistant to shoulder-surfing attack, as they select the passfaces using mouse clicks.

Fig 1. Pass faces Personnel (source: www.realuser.com)

Raj et.al. [16] proposed a novel cognition or recognition based graphical authentication scheme which is resistant to shoulder-surfing problem. Like Passfaces[14], their scheme is also based on several rounds of challenge-response protocol and users have to remember only the passicons in the sequence that forms a password. In a challenge, the user must recognize his or her password icons, or "pass-icons," out of a much larger number of randomly arranged non-pass icons. The user responds to the challenge by entering the position of the passicon by numerals (0 to 9). Several such challenges are presented in sequence, and if the user responds correctly to everyone then the user is authenticated. Using game-like approach, their scheme was designed to motivate the users to log in quickly and accurately. This shceme was improved by Bindu [17], with 4 sub-groups of icons as shown in Figure 2 and observed to be more efficient than the one with single set of icons. Thus, it infers that the users can remember easily icons which are familiar to them and of different groups.

Fig 2. Four sub groups of Passicons proposed by Bindu[17]

In recall based passwords user has to draw a unique picture for authentication in 2D grid during registration phase. During authentication user should produce or draw the same picture then only user is authenticated.

Jermyn, et al. [18] proposed “Draw - a - secret (DAS)”, which allows user to draw his/her unique password (Figure 3). A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. If the drawing touches the same grids in the same sequence, then the user is authenticated. Jermyn, et al. suggested that given reasonable-length passwords in a 5X5grid, the full password space of DAS is larger than that of the full text password space.

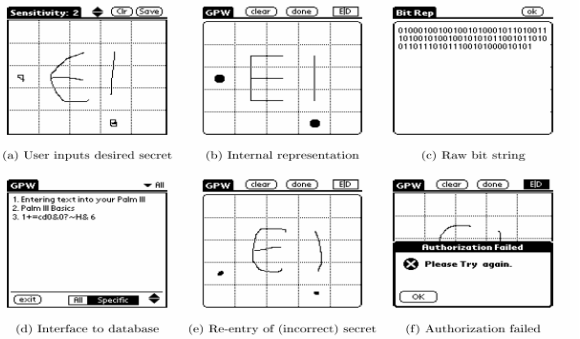

Fig 3. Draw-a-Secret (DAS) technique proposed by Jermyn, et al.[18]

Yampolskiy [19] has identified and discussed the shortcomings of various passwords techniques. Alphanumeric Passwords suffer from guessing, dictionary and brute-force search attacks. Short comings of Graphical passwords include shoulder surfing attacks, difficulties for the people with impaired vision and for the people having motor control problems. Yampolskiy has proposed PassText scheme, a new approach to user authentication that addressed some of the limitations of contemporary password schemes both graphical and textual. PassText [19] makes a strong password with few changes done by user on text file.

User authentication with PassText is promising task to adopt it in web based applications to work with text files or transferring the text files from client to server. This paper extends the PassText Scheme for authenticating the users to the Remote System. This scheme generates the password by hashing the sequence of characters obtained by concatenating the indexed numbered characters from each line of the pass text file after making the changes. Thus it offers strong security and it cannot be broken as the adversary has to identify the pass text file, changes made to the file as in case of PassText scheme and additionally he should also provide the index number. The proposed scheme is also resistant to network based vulnerabilities such as replay attack, stolen verifier attack, shoulder surfing attack etc.

The rest of paper is organized as follows: section 2 reviews the PassText Scheme proposed by Yampolskiy [19], section 3 proposes a secure usable authentication using passtext and section 4 analyzes the proposed scheme in terms of usability and security and finally section 5 concludes the paper.

II. Review Of Passtext Scheme

In this section, we review the PassText scheme proposed by R. V. Yampolskiy et al. [19]. In Textual passwords the user needs to remember the pass phrase or strong password for long term. But in the passtext authentication system user need not have to remember any passphrase or any text at all. User only needs to memorize the sequence of changes that he or she makes to the text document. Working with documents is very easy because most of the computer users work with documents frequently. Passtext is password created from a text file or set of text files by making small changes in the document. Here, User need to remember the changes been made to the text file. Basically, the author proposed three ways to provide text files to the user.

i. Providing common text file for all users is a default option. For example the Declaration of Independence can serve as a widely known base text document.
ii. User can select any text file from a list of possible base text files. This technique is more secure.
iii. Providing user’s own base text file is another option. But this might be a problem for login from remote systems.

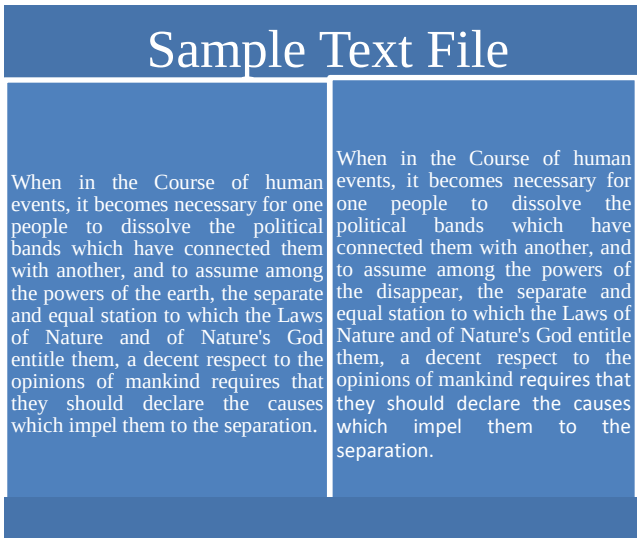

Fig 4. Sample text file with and without modifications
Left: Original base document; Right: Passtext (modified document)

To produce the PassText password user needs to do atomic modifications to the base text. Atomic modifications include typing any character or deleting any character or replace existing with the new one or combination of all these to produce a unique PassText. For example the word in the text file “earth” can be modified as “disappear”, which is simpler to remember than alpha numerical passwords as shown in Figure 4.

III. Strong Passtext Password For Remote User Authentication

A secure usable user authentication method by obtaining a strong passtext password from the text file which is chosen by the user is proposed in this section. In this proposed scheme, the user registers himself with the system with a user id and selecting a file from among several files stored in the database and few changes are made to the document, and then the user selects an index number. The indexed value letters in the words of modified document is concatenated to form the password which is hashed and stored at the server. As the user makes the change to the retrieved text file and also it is combined with selecting the characters in the index valued letters in each word of the modified text the password becomes very strong, but the user has to remember only the changes he made to the text file and the index position. Guessing of the password also becomes difficult as the attacker has to learn both the changes made to the text file and the position and he will not be able to retrieve the password directly as it is random in nature (concatenation of index numbered letters of the words). Thus usability and security of the system is enhanced with this proposed scheme. Figure 5 shows retrieving of the text file from server database by administrator. This scheme has been extended to provide authentication between the client and the server.

The notations used in this paper are as follows:

U: The user.
ID: The user Identification.
S: Server system.
PW: The password of user U.
h (.): A one way hash function.
E(y, x): encryption of y with key x
D(y, x): decryption of y with key x

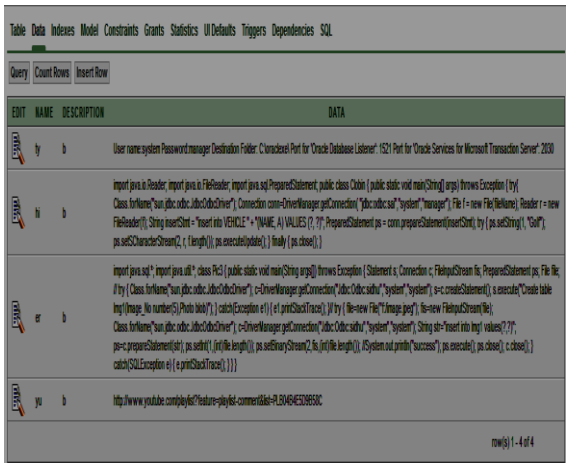

Fig 5. Retrieving .txt files from server

There are three phases involved in the remote authentication process.

A. Registration phase:

This phase is executed only once at the time of registration. The steps involved in registration phase are:

Step 1. User chooses a user id.

Step 2. User selects one of the files among multiple files from the server or their own text file. User is presented with the .txt file and needs to change the document like add the text, delete or replace the words in the selected file. Then the user selects an index number to create unique strong passtext password by combining the index numbered character in each line of the modified document.

Step 3. The original document will be saved in the server in a CLOB format for future purpose and the strong passtext password is hashed and stored in the database at the server against the user id.

B. Authentication phase:

This phase involves two sub phases: Login Phase and the verification phase and will be executed every time a user wants to login to the server.

a. Login Phase:

Step 1. User enters the user id and sends to the Remote System.

Step 2. System sends the associated text file according to the user ID and a random challenge (nonce) x.

Step 3. User needs to do the same modifications to the file as done in the registration process.

Step 4. User needs to enter the index value to obtain random unique strong PassText password (pw) from text file by concatenating the indexed numbered character in each line of the modified text.

Step 5. User encrypts the password (pw) with the random number x and sends it to the Remote System.

b. Verification Phase:

Step 1. System decrypts the encrypted password by random number x.

Step 2. Now, the decrypted PassText password is hashed, compared with the password hash stored against the user id in the database and if it is matches the user is successfully authenticated to the system.

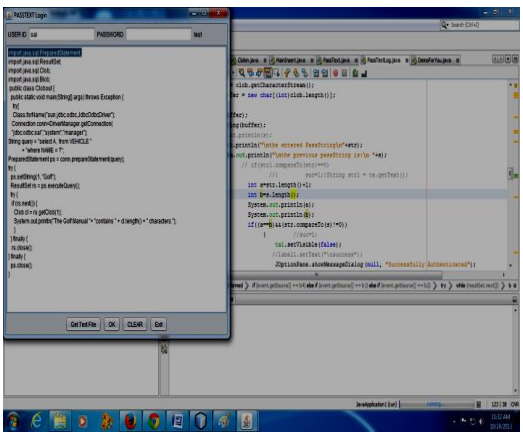

Fig 6. System prompts .txt file to prove identity after user provides the User Id at the time of login

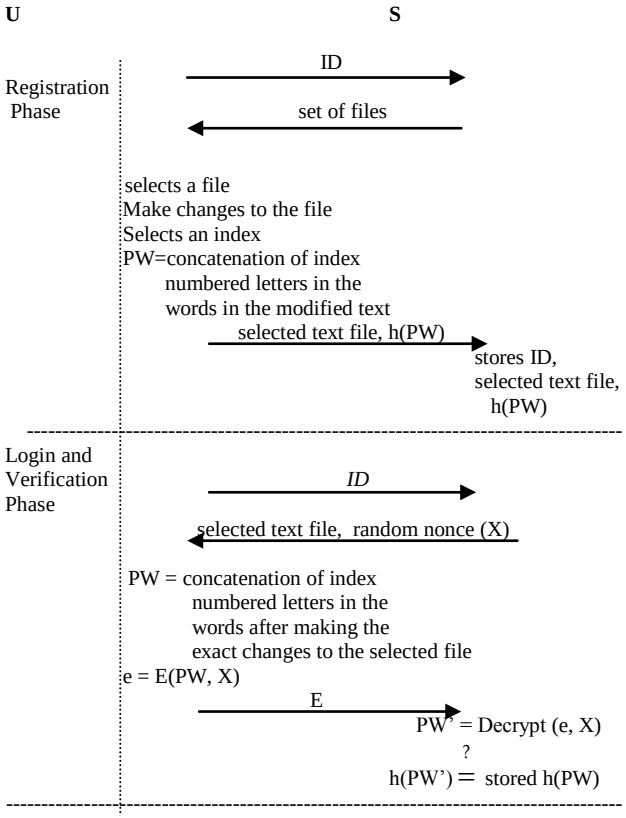

Fig 7. Registration and Login and verification phase of the proposed scheme

C. Password change phase:

Users have the freedom to change his or her password as follows:

Step 1. User should prove himself or herself as authorized user as similar to login phase.

Step 2. Now, an authenticated user can change passtext password same as in the registration process.

Step 3. The original document in CLOB format and strong passtext password is hashed and stored in the database for future login.

IV. Usability And Security Analysis Of Proposed Scheme

This section deals with the usability and security aspects of proposed scheme. Security refers to how authentication methods counter various attacks. Usability refers to the degree to which password is easy to use with no training.

A. Security analysis

The proposed scheme is secured against various vulnerabilities as follows:

a. Secure against guessing attack

It is more difficult for the attacker to know what modifications have been done to the base document. So, it is secure against guessing attack.

b. Secure against brute force search attack

Suppose if the user has chosen the text file of size 64k with three modifications done the password space [20] becomes$(2^{16})^3$. So the proposed scheme is resistant to brute force attack even with small changes in the file makes a strong password.

c. Secure against dictionary attack

There is no dictionary for what the user has modified in the base document. So, it is difficult to carry out dictionary attack compared to classical passwords.

d. Secure against Shoulder-surfing attack.

This is the process of observation of login of authorized user over his or her shoulder by an adversary. Compared to other graphical passwords it is less vulnerable to shoulder-surfing attack [21], because usually the observer can remember pictures easily than the modifications to the text. Even though the changes made to the document by the user are viewed by the attackers, he will not be able to identify the index number given by the user as will not be displayed on the screen. So, the proposed scheme is secured against Shoulder-surfing attack.

e. Secure against Spyware attack

This is a key logger [22] or key listening technique to obtain the password. It is very hard to crack the graphical password by key listening. In Proposed system, we type only the changes and the index number. Sometimes we delete the data using mouse and keyboard. Key loggers can record all that is typed but the changes made have to be viewed by the user in synchrony. This reduces the chance of the password being revealed and hence is secure against Spyware attack.

f. Secure against replay attack

For every login a new random challenge (nonce) is used, the adversary will be identified if he replays the message intercepted in the previous login session.

g. Secure against stolen verifier attack

As the password is formed by concatenating the characters at an indexed number in each line and then hashed, even when the attackers gets hold of the verifier table he will not be able to learn the password because of its randomness.

B. Usability of the system

The proposed scheme is tested with the help of 50 novice users from the campus who are unaware of the scheme and all the usability aspects are reported below.

a. Time taken for Registration:

The basic thing for any authentication scheme is the registration time, where user registers themselves with the proposed scheme while registering the users are prompted to make three changes to the original document and the time taken to register by the 50 users are depicted in figure 8.

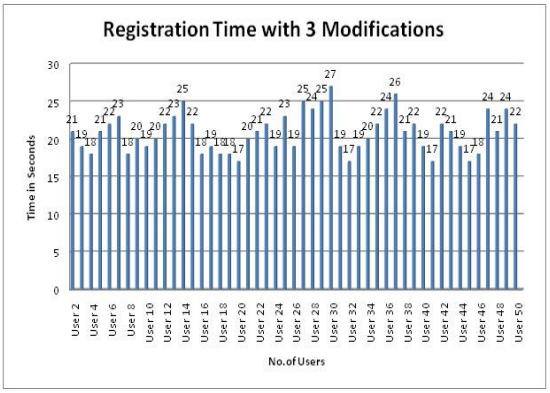

Fig 8. Registration time of 50 users

As we can see the maximum time taken to register is below 30 seconds.

b. Time taken for Login:

Coming to the Login time of the 50 users, the proposed scheme is tested for a week first the users are asked to login immediately after their registration and the login time for immediate login are depicted in figure 9:

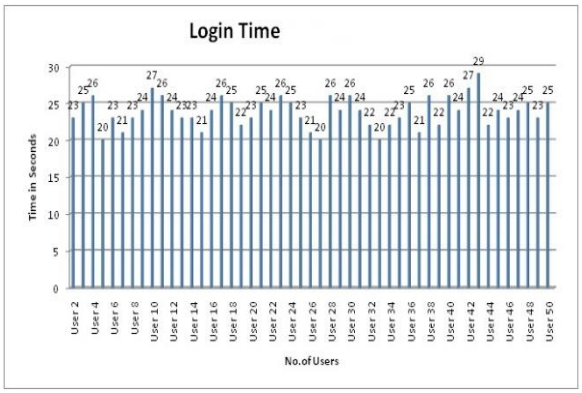

Fig 9. Login time of 50 users immediately after registration

As we can observe the maximum time taken to login is 29 seconds.

After a week the users are requested to login again in order to test their memorability and the login time are recorded as well and the same are depicted in figure 10.

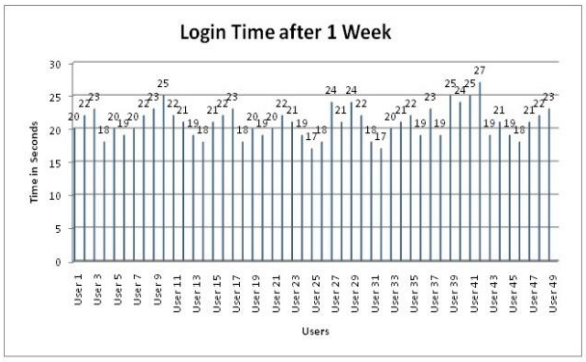

Fig 10. Login time of 50 users after a week

If we observe the time taken to login after a week is 2 seconds less than the time taken to login after immediate registration. It implies that the users could able to remember the changes made to the text file better and that they have got familiarity with the system.

c. Number of mouse clicks:

Another aspect of the usability study is the number of mouse clicks user used throughout his/her experience with the proposed scheme. Even the mouse clicks are registered and depicted in figure 11:

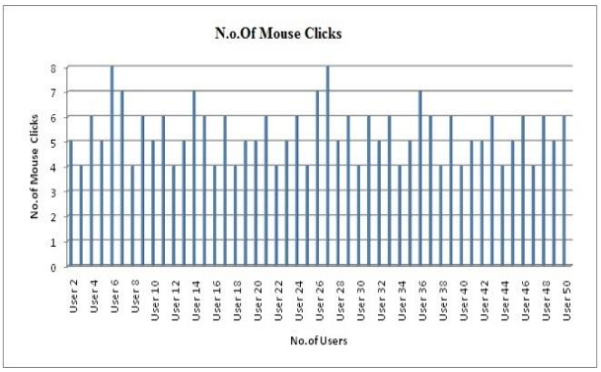

Fig 11. Number of Mouse clicks used by 50 Users

So throughout their experience with the proposed scheme users used maximum 8 clicks to provide input. As the number of mouse clicks are minimum the usability of the system is more.

d. System Usability Scale (SUS):

The System Usability Scale (SUS) provides a "quick and dirty", reliable tool for measuring the usability. It consists of a 10 item questionnaire with five response options for respondents; from strongly agree to strongly disagree.

i. The System Usability Scale

When a SUS is used, participants are asked to score the following 10 items with one of five responses that range from Strongly Agree to strongly disagree:

1. I think that I would like to use this system frequently.
2. I found the system unnecessarily complex.
3. I thought the system was easy to use.
4. I think that I would need the support of a technical person to be able to use this system.
5. I found the various functions in this system were well integrated.
6. I thought there was too much inconsistency in this system.
7. I would imagine that most people would learn to use this system very quickly.
8. I found the system very cumbersome to use.
9. I felt very confident using the system.
10. I needed to learn a lot of things before I could get going with this system

ii. Interpreting Scores

Interpreting scoring can be complex. The participant's scores for each question are converted to a new number, added together and then multiplied by 2.5 to convert the original scores of 0-40 to 0-100. Though the scores are 0-100, these are not percentages and should be considered only in terms of their percentile ranking.

The proposed scheme is tested for SUS with help of 50 novice users using morae Tool which is usability testing software that uses the above SUS process for calculating the Usability of the proposed scheme. Using Morae Tool the user experience of 25 users is recorded and the SUS Score is calculated for each user, figure 12 depicts the same. It can be observed that the average SUS score for the proposed system is 70, which implies that the system is very user friendly.

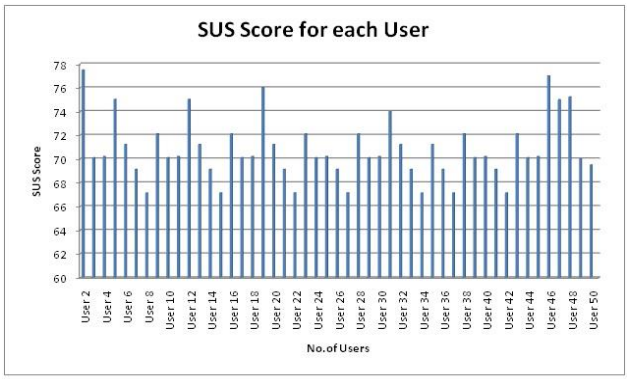

Fig 12. SUS Score of 50 users

V. Conclusion

The proposed scheme "secure usable authentication using strong passtext passwords" is easy to learn, remember with small number of changes in the Text file and it is made difficult to crack the password.

The proposed scheme defends various security attacks such as guessing attacks, shoulder surfing attack, replay attack etc. The usability of the proposed scheme is analyzed using Morea tool and it has been found that the average System Usability score is 70. The proposed system has the advantage that the user need not have to store the file used in generating the password, as it is maintained by the server, lessen the memory requirements at the user's side.

Acknowledgment

I am indebted to All India Council for Technical Education (AICTE) for providing an environment where we can work to our level best. I would also like to thank all the Usable Security Lab scholars for their help in carrying out this work.

References

[1] J.-C. Birget, D. Hong and N. Memon, *Robust Discretization with an application to the Graphical Passwords,Availableat:citeseer.ist.psu.edu*/birget03robust .htm Retrieved November 4, 2005.

[2] K. Renaud and E. Smith, *Jiminy: Helping Users to Remember Their Passwords*, *Annual Conference of the South African Institute of Computer Scientists and Information Technologists*, Pretoria, South Africa, 25-28 September 2001.

[3] A. Brostoff, *Improving Password System Effectiveness*, *PhD Dissertation*, Department of Computer Science University College London, September 30, 2004.

[4] N. Provos and D. Mazieres, *A Future-Adaptable Password Scheme*, *USENIX Annual Technical Conference*, Monterey, California, USA, June 6-11, 1999.

[5] R. Morris and K. Thompson, *Password Security: a Case History*, *CACM*, 1979, pp. 594--597.

[6] K. Renaud, *Quantifying the Quality of Web Authentication Mechanisms. A Usability Perspective*, *Journal of Web Engineering*, *Volume 3 Issue 2*, October 2004.

[7] Julie Thorpe, P. C. van Oorschot, Anil Somayaji, Pass-thoughts: authenticating with our minds, Proceedings of the 2005 workshop on New security paradigms, September, 2005, Lake Arrowhead, California.

[8] E. Bekkering, M. Warkentin and K. Davis, A Longitudinal Comparison of Four Password Procedures, Proceedings of the 2003 Hawaii International Conference on Business, Honolulu, HI, June 2003.

[9] Min-Shiang Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 46, no. 1, pp. 28-30, 2000.

[10] Das M. L., Saxena A. and Gulati V. P., "A dynamic ID-based remote user authentication scheme", IEEE Trans. Consumer Electronics, May 2004, vol.50, No. 2: 629 -631.

[11] C. Shoba Bindu, P. Chandrasekhar Reddy and B. Satyanarayana, "Improved remote user authentication scheme preserving user anonymity", International Journal of Computer Science and Network Security, vol. 8, no. 3, pp. 62-66, March 2008.

[12] Ajay Sharma, Deo Brat Ojha, "Password Hardened Biometric: A Complete Solution of Online Security", International Journal of Computer Network and Information Security, 2013, 6, 42-48, DOI: 10.5815/ijcnis.2013.06.06

[13] G. E. Blonder, Graphical Passwords, United States Pattent 5559961, 1996.

[14] Pass Faces. Corporation, 2009 *The Science Behind Pass faces*, *White paper*, http://www.passfaces.com/enterprise/ resources/white_papers.htm.

[15] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proceedings of the 13th Usenix Security Symposium. San Diego, CA, 2004.

[16] Raj Mohammed, C. Shoba Bindu, P. Chandrasekhar Reddy and B. Satyanarayana, "A novel cognition based Graphical Authentication scheme which is resistant to shoulder-surfing attack", in Proceedings of 2nd International conference on information Processing, ICIP 2008.

[17] C. Shoba Bindu, "Improved novel graphical password authentication scheme and usability study", i-manager's journal of Software Engineering, Vol. 3,No. 4, April- June 2009.

[18] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.

[19] R. V. Yampolskiy,"Secure Network authentication with PassText", The IEEE International conference on Information and Technology ITNG'07, April 2007.
[20] R. V. Yampolskiy, *Analyzing User Password Selection Behavior for Reduction of Password Space*, *The IEEE International Carnahan Conference on Security Technology (ICCST06)*, Lexington, Kentucky, October 17-19, 2006.
[21] Susan Wiedenbeck and Jim Waters & Leonardo Sobrado and Jean-Camille Birget "Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme" Proceedings of the working conference on Advanced visual interfaces, Pages 177-184. New York, USA 2006.
[22] Nairit Adhikary, Rohit Shrivastava, Ashwani Kumar, Sunil Kumar Verma, Monark Bag, Vrijendra Singh, "Battering Keyloggers and Screen Recording Software by Fabricating Passwords" , International Journal of Computer Network and Information Security, 2012, 5, 13-21, DOI: 10.5815/ijcnis.2012.05.02

Authors' Profiles

Dr. C.Shoba Bindu is an Associative Professor & Head, Department of Computer Science & Engineering at Jawaharlal Nehru Technological University college of Engineering, Ananthapuramu. She obtained her Bachelor degree in Electronics and Communication Engineering, Mater of Technology in Computer Science from Jawaharlal Nehru Technological University Hyderabad & Ph.D. in Computer Science & Engineering from Jawaharlal Nehru Technological University Anantapur. She has published several Research papers in National\International Conferences and Journals. Her research interests includes network security and Wireless communication systems.

How to cite this paper: C. Shoba Bindu,"Secure Usable Authentication Using Strong Pass text Passwords", IJCNIS, vol.7, no.3, pp. 57-64, 2015.DOI: 10.5815/ijcnis.2015.03.08

