ISSN No. 0976-5697

Volume 2, No. 4, July-August 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Improved Cognition based Authentication Scheme Using PassScript

Raj Mohammed Mohd*
Deparment of .C.S.E,
VITS-SET,
Karimnagar Andhra.Pradesh,India
raaz.mohd@gmail.com

Dr. C.Shoba Bindu
Deparment of .C.S.E,
JNTUCE,
Anantapur, Andhra.Pradesh,India
shobabindu@gmail.com

Dr. D.Vasumathi
Deparment of .C.S.E,
JNTUCE,
Hyderabad, Andhra.Pradesh,India
vasukumar_devara@yahoo.co.in

Abstract: The fundamental goal of the usable security research is providing the usability to the user without compromising the security of the system. This paper discusses a novel cognition based graphical authentication method, which is resilient against to shoulder-surfing attacks proposed by us [16]. In this paper, we have used the regional script Telugu as Password instead of Pass icon in order to improve the usability of the user. This paper mainly focuses on the people, who know their regional language and not universal language. It also enhance the security of the system by avoiding different kinds of attacks on Passwords. We compare and analyses proposed scheme with existing schemes. This paper gives a momentum for the Usable security with User's persuasion taken in to consideration.

Keywords: Cognitive Passwords, User Authentication, PassScript, Usability and Security

I. INTRODUCTION

Authentication is process of determining the whether the user can allow to access the system or resource. The most common authentication method is for user submits the username and password or PIN number to authenticate the system as authorized user. A cognitive password is a form of knowledge-based authentication that requires a user to answer a question, presumably something they intrinsically know, to verify their identity. Cognitive password systems have been researched for many years, and are currently commonly used as a form of secondary access. Some of the researchers have gone for two factor authentication to enhance the security by means of biometrics and smartcards. But, these are expensive in use.

The vulnerabilities of this method are well-known. One of the problems of this method is difficulty of remembering the passwords for long term memory (LTM).Usually, the users are tending to chose small, simple and short and dictionary words as passwords. But, these are vulnerable to dictionary, brute-force shoulder-surfing and guessing attacks etc. Some times, user tends to choose the strong password which is composed of alphanumeric with small and capital letters which is hard to guess and crack. But, it is hard to remember. In order to solve this problem, Researchers had gone for graphical authentication systems are proposed as an alternative to text based password schemes to improve the usability and security issues. In a typical graphical authentication scheme user chooses pictures as his or her password at the time of enrollment stage. When logging to the system, user need to chose the correct sequence of pictures as password by recognizing the previously chosen images or pictures as password. Human beings are[10] good at recognizing the faces, icons and pictures rather than random strings or words. In 1996, G.E.Blonder introduced graphical password approach in which user click on the predefined points on the images or pictures in a sequence to generate the password for the authentication. These are easy to remember and may be difficult to crack by means of automated tools. Even though, they are resistant to brute-force and dictionary attacks because of their large password space. However, Graphical passwords are suffering from shoulder–surfing attack, which becomes severe when applying to various business applications on networks and banks etc.

We proposed a novel cognition based graphical password scheme [18] which is designed by Challenge-Response Protocol and also depends on the cognizance of the user to select the PassIcon from hand hidden keypad. This scheme is also resistant to shoulder-surfing, brute-force attacks and has less chance for guessing attack. This scheme can be applied to the ATMs, PDA s and Mobile devices.

The limitation of our previous work is that the user is unable to remember the passicon which is not having any visual cue to remember for long term. So, we introduced a PassScript which is related to regional language to improve the memorability and it also easy to use by the people who doesn't know the English. This scheme helps the people who has belongs to their region.

The rest of the paper organized as follows: In Section 2, we review the Cognition based authentication schemes, Section 3 describes the proposed scheme, and Section 4 analyzes and compare with various cognition based scheme with the proposed scheme, finally conclude in Section 5.

II. REVIEW OF COGNITION BASED AUTHENTICATION SCHEMES

In this section, we review the cognition based authentication methods can be classified in to three categories; one- textual Passwords, Second -graphical

passwords ([5], [6]) which are alternative to textual passwords and the other one is Visual Cue Script Passwords. Textual passwords almost vulnerable to all kinds of attacks by an adversary. But, graphical passwords will increases the usability and security of the system. These schemes are classified in to three types: one- Cognition based graphical passwords, two- Position based graphical passwords and the other Recall based graphical passwords.

In Position based authentication scheme, User need to select the sequence of positions on the image in a sequence to form a password. In 1996, G.E.Blonder [5] was first introduced graphical password scheme by selecting the pre-defined positions on the image as a password. This scheme has a problem of clicking the exact position of an image and violates the usability of user. This is also not resistant to shoulder surfing. The password space for this is more as compare to the cognition based a graphical password that is N^K. Where N is number of pixels or smallest units of picture and K is the number of locations to be clicked on as password.

Pass Point Systems, a popular position based or cued recall based method and proposed by Wiedenbeck et al. [8]. In this scheme, User need to tolerance of image or 20X20 pixels as one pass point in order to achieve user flexibility to click on the image. The user needs to select any where on the tolerance region of image to authenticate the system or resource. These position based schemes are not resistant to guessing, brute-force and shoulder-surfing attacks.

The recall based Authentication schemes are based on the recalling of the procedure which has been done at registration phase. User can draw on the grids to authenticate the system. It occupies the infinite password space to store the password sequence in the form of co ordinate points {(1, 4) (2, 3) (4, 6),(6.9)}.In this scheme, user may fail to remember the sequence of drawing in terms of curves which are random.

Jermyn et al. [15] proposed a Draw A Secret (DAS) scheme which provides the users to draw some thing on the grids with some strokes. The password space is large as compared to textual passwords.

Because of the fewer strokes for fixed password length decreases the password size. This is not resistant to shoulder-surfing and dictionary attacks. Syukuri et al. [9] proposed a DAS scheme which is easy to remember and occupy infinite password space. The user can draw the signature of own instead of drawing zig-jag curve. So, it is not resistant to guessing attack. Most of recall based methods are not resistant to Dictionary attacks and shoulder-surfing attacks.

In Cognition based Passwords, the user need to select the sequence of images or pictures from portfolio of images or pictures to authenticate the system. PassFaces[1] is the first and most well-known recognition based authentication approach which is launched by real user corporation. This scheme relies on the ease of remembering the faces of familiar ones. User will select the face which is familiar from the images at the stage of enrolment. This process is repeated with five times with 3x3 grid results a small space of 59050 possible face combinations. This scheme is vulnerable to Dictionary attack, brute-force,guess and shoulder-surfing attack.

Another Cognition based authentication scheme Déjà vu [3] is based on random art. User need to choose five images as pass set and during the authentication he or she need to select his/ her pass set from a challenge set of 25 images. Since, these are completely random and generated by computer program. It's difficult to share the Déjà vu password with others. But, it consumes more login time as compared to textual passwords.

Jansen et al. [14] proposed an authentication scheme with thumbnail images which is useful to handheld devices such as Mobile devices, PDAs and Gizmos. The number of pictures is less (30 in number) in order to incorporate in the small storage devices. The password space for this is same as Pass Faces. This scheme is vulnerable to brute-force search, guessing and shoulder-surfing attacks.

Takada and Koike proposed a graphical authentication scheme, which is similar to Jansen et.al scheme. User can select his favorite images rather than computer generated random images. The problem of this approach is the difference between various kinds of images may become a guess to an adversary. The password space is $(N+1)^K$. where K is number of rounds of verification and N is the number of pictures. It is also suffers from brute force, guessing and shoulder-surfing attacks.

All of the above-mentioned schemes are vulnerable to shoulder-surfing attack that is process of observing the login of authorized user or recording the login by hidden cameras. An adversary can enter in to the system just by observing the images selected by the authorized user. In order to solve this problem, Birget proposed shoulder-surfing resistant graphical authentication scheme [7] by using Convex Hull or Triangle scheme. It is also suffers from brute-force search and guessing attacks. This scheme suffers from edge problem and rendering the more objects on the screen at first time takes time. The password space of this scheme is C(N,K).where N is total number of picture objects and K is number of pre-registered passobjects.

Man et al., [11] proposed an authentication scheme which adds the graphical layer to the text based passwords and strongly resistant to shoulder surfing. But, this scheme vulnerable to guessing attack and brute-force attacks. However, the user needs to remember both the text password and graphical images which are used for the authentication. The login process of the protocol takes longer time distinguishes various variations which are used for one passicon.

All of the above mentioned schemes are designed using challenge-response protocol to enhance the security by sharing the secret between the user and the system. Roth et al.'s [4] scheme makes PIN-entry shoulder-surfing resistant to a limited degree. The limitation of this scheme is that an attacker can figure out the PIN given full information about the questions and answers, for example, if the attacker has an excellent memory or records the login. Observing multiple logins in which the attacker could accumulate more knowledge about the PIN that would eventually determine it would further facilitate an attack.

These limitations may be acceptable because the attacker must have both the token and the secret PIN to gain access. Note that this differs significantly from authentication by passwords, where there is no token and the secret is the only defense against unauthorized access. Consequently, passwords should be stronger (longer and from a larger set of characters or images).

In order to solve the shoulder-surfing problem in graphical passwords, we propose a novel cognition based graphical authentication, which is resistant to shoulder-surfing attack. But, we observed that user felt difficulty to remember the sequence of passicons. So, we propose one more solution to improve the memorabiity of the user.

III. AUTHENTICATION USING PASSSCRIPT

Our Novel shoulder-surfing resistant cognition based authentication scheme, which is resilient against shoulder-surfing attacks by human observation, video recording, or electronic capture. Like Passfaces [12], this scheme is based on several rounds of challenge-response protocol and users should remember only the letters (in the form of pictures) in a sequence that forms their password. In this scheme, the graphical elements used in authentication are letters shown in a window on the screen. In a challenge the user must recognize some minimum number of his or her password letters, or "pass-script," out of a much larger number of randomly arranged Non-passscript letters. The user responds to the challenge by entering the position of the pass script letter where it is situated on window (0….7). Several such challenges are presented in sequence, and if the user responds correctly to every round then the user is authenticated. Using a game like approach, this scheme is designed to motivate the users to log in quickly and accurately.

The system uses a large portfolio consisting of several hundred icons. In our implementation the icons used were all icons of software applications, but the portfolio of icons could be any kind of small icons, even user-provided ones. The icons are displayed using only the image without text. To create a password the user chooses several icons from the portfolio to be his or her pass-script letters (Figure1). The user has to remember only the pass-icons in a correct sequence he or she selected. Therefore, it is advisable for the user to commit them to memory and practice using them. At login time a large number of icons from the portfolio are randomly arranged in the password window. These icons include mostly decoy icons along with a one pass-icon for each screen. The login takes place in a series of challenge-response rounds. The number of rounds is the number of passicons selected by the user, so this is easily changed, with more rounds providing higher security.

When the login begins, the user must visually locate one passicon for one window and the user's next step is to know the position where it is situated at that instant. After that, user should enter the row and column of the passicon where it is situated.

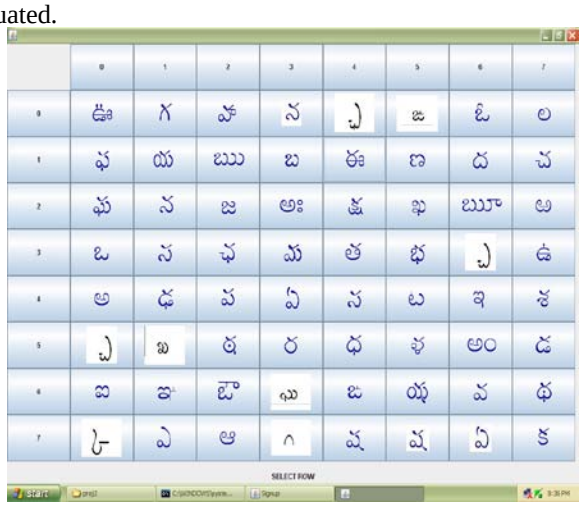

Figure. 1. Cognitive Password window Regional Script (Telugu)

Specific information about the location of the error. Beyond its shoulder-surfing resistant properties, there are three main considerations about the security of this scheme. First, the password space can be made very large, and therefore more secure, by increasing the number of Non-passscript letters, the number of passscript letters, or both.

The size of the window is 8x8 grid consists of 64 passscript letters for every round and the ability of users to locate their passscript letters among a large number of icons. Second, a brute-force attack is infeasible. An attacker could try to get all possible passwords with their position can be changed time to time observed by shoulder-surfing. After successive observations, the attacker could rule out more and more passwords.

However, eventually the attacker would have to record a significant portion of all possible passwords, which would require far too much memory. Third, using challenge-response protocol, there is always the possibility of accidental login (i.e., an attacker could type correct position with a probability of 0.01). This is different from guessing the password. To make accidental login unlikely we do three things:

A. Passcript, which in the form of pictures will be randomly placed in the window so that the user has the same probability of being to guess one pass-script which is part of his or her password.
B. The position can be varied within fraction of seconds in large window after entering the position of the passscript.
C. To log in, the user has to respond to multiple challenges equal to length of the password he/she has chosen. User traps the eye-tracker to guard the password as secure from mapping the user sight while locating the passicon from the window and, at least in some cases, discover the pass-icons. We consider this a potential threat, not an imminent threat, because current eye-trackers cannot be used without being detected by the user.

To guess the password, the adversary needs to select one passicon per one round so, there is probability to obtain the password for one round is C (64,1) and it can be hard to guess for more number of rounds equal to length of the password chosen.

The usability of the user will increase by seeing the position of passicon from an attractive window which consists of 0 to 7 grids displayed to get the position easily by seeing the passicon as rendered in the figure1.

IV. USABILITY & SECURITY ISSUES OF THE PROPOSED SCHEME

In this section, we have analyzed proposed scheme with usability and security issues and also compared with existing schemes previously proposed

A. Usability of Participants

Ten novice users, who were unfamiliar with this scheme, were taken from a university campus. The participants were experienced computer users who reported using computers for at least 6 hours per day for work and personal activities. The set of software application icons was used. The number of icons rendered in any challenge is 64. During a login the desired pass-icon will be displayed on window random position by the system for every challenge. The number of non-pass-icons, pass-icons, and challenges will affect the security concerns. The system also provides the user to select the row and column of the passicon easily by means of the row and column numbers as rendered on the window. We had given the guidelines to the participants to use the system in an effective way.

B. Procedure & Results

Participants carried out the usability study individually in two sessions, an initial session and a follow-up session 5 days later. In the first session the participants are interested to learn about the system with questionnaire. Next the experimenter explained the purpose of the system and how it worked, using the power point presentation. The experimenter explained the concept of this scheme using Figure1.The experimenter also instructed the participant not to use the mouse to select pass-icon and instructed to choose them with hand hidden keypad which is provided to them. To avoid the eye tracking, user is instructed to see on other passscript while entering the position of the Passscript. The experimenter explained to the user that feedback on correctness would be given only at the end of the whole password input, not between each of all the challenges. The participant authenticated him by measuring time for each correct and incorrect login and challenge. The authentication trials took about 10 minutes.

All participants achieved the criterion of correct login with a new average login time of 54 seconds to authenticate the system successfully with 5 passscript letters. The mean time for correct password inputs was also analyzed that is main factor for the usability of the user. In the observation; there was a gentle downward trend in time to input the password. Most of the users are satisfied with icons that are displayed on the window to choose the password.

Table I. Probability of Password guessing per one round & login time of user.

S.No	*Name of scheme*	*Probability of guessing the Password/ one round*	*Login time*
1	PassFaces	0.11	20 sec
2	Déjà vu	0.04	30 sec
3	Man et al.	0.22	---
4	Convex Hull click	---	72 sec
5	Proposed scheme with Pass Icons	0.01	64 sec
6	Proposed scheme with Regional PassScript	0.015	54 sec

C. Security Issues

This scheme is vulnerable to shoulder-surfing attack, brute-force, guessing and dictionary attacks which are associated with graphical password schemes in more general.

a. This scheme is vulnerable to dictionary attack. Because, passcript stored as the pictures which are stored by occupying more storage space. There is no dictionary information regarding the pictures.
b. This is resistant to brute-force attack because, there are no automated tools to crack the password. So, this scheme is resistant to brute-force search.
c. This scheme may also resistant to social engineering attack that is user unable to reveal the password through a mobile.
d. This scheme is resistant to shoulder-surfing attack by using the procedure, which has been done by hand-hidden keypad to enter the position of the passscript, which are randomly changes in the window. Even if an adversary observes the movement of fingers while typing the row and column of the passscript he can't guess the picture password that is set of the passscript.
e. This scheme also resistant to guessing attack passscript are placed random on 8X8 grid. An adversary unable to guess the password 1 out of 64 letters of pictures and length of password which varies with one round to another becomes more complex to guess the password.

D. Comparison:

We compare various cognition-based techniques with our proposed scheme. The probability of guessing the password per one challenge that is one round is listed as fallows in chart. Our proposed scheme has only probability of 0.015 that is very less compared with previous schemes and also login time of various schemes s displayed on a table1.

V. CONCLUSION

In this paper, we have proposed a novel cognition based authentication scheme, which is resistant to shoulder surfing that can be severe attack of graphical passwords. This scheme can be deployed with regional passscript letters to improve the usability of the user. This scheme can be applied to small storage devices like PDAs, Mobile devices and also useful to ATMs with hand hidden keypad to enter the position of the passscript letter. This scheme is applicable to the systems where the keypad is covered to the shoulder-surfer and also used for remote user authentication to increase the usability. This scheme reduces the login and registration time of the user as compared to our previous scheme.

VI. ACKNOWLEDGMENT

We are thankful to the participants who are participated in the usability study of the proposed system.

VII. REFERENCES

[1] Brostoff, S. and Sasse, M.A. Are Passfaces more usable than passwords: A field trial investigation. In McDonald S., et al.(Eds.), People and Computers XIV - Usability or Else, Proc. of HCI 2000, Springer, 2000, 405-424.
[2] Davis, D., Monrose, F., and Reiter, M.K. On user choice in graphical password schemes. In Proc. Of the 13th USENIX Security Symposium, San Diego, 2004.
[3] Dhamija, R. and Perrig, A. Déjà Vu: User study using images for authentication. In Ninth Usenix Security Symposium, 2000.
[4] Roth, V., Richter, K., and Freidinger, R. A PIN-entry method resilient against shoulder-surfing. Proc of the 11th ACM Conference on Computer and Communications Security, 2004, 236-245.
[5] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed.United States, 1996.
[6] Xiao Yuan Suo Ying Zhu G. Scott. Owen "Graphical Passwords: A Survey".
[7] Sobrado, L. and Birget, J.C. Graphical passwords. The Rutgers Scholar, 4, (Sept. 2002).http://RutgersScholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm.
[8] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., and Memon, N. PassPoints: design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies, 63, (2005), 102-127.
[9] A. 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): Springer-

Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441

[10] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.

[11] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003.

[12] T. Valentine, "Memory for Passfaces after a Long Delay," Technical Report, Goldsmiths College, University of London 1999.

[13] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices," National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.

[14] 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.

[15] S. Wiedenbeck, J. Waters, J. C. Birget "Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme" AVI '06, May 23-26, 2006, Venezia, Italy.Copyright 2006 ACM 1-59593-353-0/06/0005.

[16] Raj Mohammed,C.Shoba Bindu " A Novel Cognition based graphical authentication scheme resistant to Shoulder-surfing attack". ICIP'08.