International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 05
April 2017

Constrain Identification Resistant Graphical Authentication Scheme

K. THOLI SANDHYA, P. S. NAVEEN KUMAR
PG Student, Dept. of MCA, St. Ann's college of Engineering &Technology , chirala.
Assistant Prof, Dept. of MCA, St. Ann's college of Engineering &Technology , chirala.

Abstract: *Graphical scheme is commonly used for authentication but this scheme is vulnerable to dictionary attack, shoulder surfing attack, accidental login. Hence the text-based shoulder surfing resistant graphical password schemes is proposed. This proposed system based on partially identification attacker model is partially observe the login procedure. Classical PIN entry is a popular scheme is greatly balances the usability as well as security aspects of a system. .A personal identification number (PIN) entered in to numeric password in mobile and stationary systems. The Shoulder Surfing Attack (SSA) becomes great unease. The Session key mechanism is proposed the proposed system introduces number of Virtual Random Keyboard and a secure intellectual OTP and LTP methods for securing the authentication at a higher level. Thus the proposed system provide user securely login without any attack probability by multiple level security and advanced attack preventing system. Our results demonstrate that gaze-based password entry requires marginal additional time over using a keyboard error rates is similar to every keyboard and subjects preferred the gaze-based password entry approach over traditional methods.*

Index Terms: OTP, Password Attacks, Graphical Password, Shoulder Surfing Attack, Validation,Hashfunction,Classical PIN, Partially Observe

.

1. INTRODUCTION

Passwords remain the dominant means of authentication in today's systems because of their simplicity [1] legacy deployment and change revocation. Unfortunately common model to entering passwords using keyboard mouse, touch screen or any traditional input device is frequently vulnerable to attacks such as shoulder surfing keyboard acoustics [2,3], and screen electromagnetic emanations. Major aspect that actually impact significantly in real life is usability

GUI design models and strategies may intentionally unintentionally many users tendency behavior modify less secure transactional behaviors constraints based on essential research work considering the capabilities and shortcomings of the targeted users. In pictorial passwords human inclination for retaining visual [4] passwords is encourage the ideal determination and proper utilization of exceptionally secure and passwords that have less consistency ceasing clients from risky practices [5] some distinct datasets is created for attacks using the dictionaries relevant to the recent data in the users login model collected from many sources other than the actual target sources and the other based on recognition of click-order model. Once the evaluation and analysis of the both the datasets is completed validation is carried out to study the user click patterns and recognize the user passwords using this attack [6]..

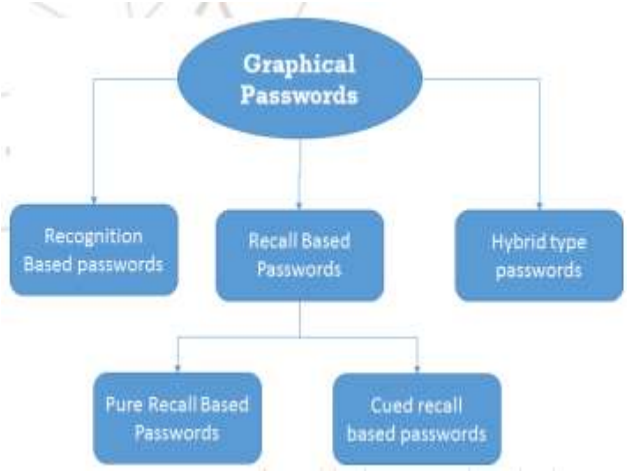

Figure 1: Types of graphical password methods

2. RELATED WORK

Sobrado [7] proposed shoulder surfing resistant method triangle scheme movable frame, and intersection scheme. In triangle scheme is randomly spread the N number of object and user has to select the pass object as his password which is selected previously to login into the system. User must select the pass object and has to click inside the invisible triangle created by those objects. Our system is support observable schemes which have motivated us to propose the Color Pass scheme for remove shoulder surfing attack [8]. In this category under the registration process of the system users need to select specific images of choice from large dataset of random images, icons or symbols. Study and analysis was done to determine accountability of memorizing passwords and it signified that recall the graphical passwords even after 60 days by the most of the users [9]. The major advantage of the OTPs over present passwords is that they reused once it has been used for the logon model. OTPS also have an additional feature of random and irregular patterns which are hard to memorize and predicted for future use [10]. In general, model to overcoming shoulder surfing rely on "increasing

the noise" for the observer so that it becomes difficult for the observer to disambiguate the user's actions/input. Roth [11] present model for PIN entry which uses the philosophy of increasing the noise for the observer In their method the PIN digits are displayed in two distinct sets colored black and white. The correct PIN digit is finding by intersecting the user take choices. The system requires users to make multiple binary selections in order to correctly input each digit of the PIN.

3. ARCHITECTURE

System architecture is the conceptual sculpt new model activities, and views of a system. An structural design description is a formal description and representation of a system, organized to supports analysis in the structures and activities of the system. System architecture is over the system components the superficially visible properties of those components [12] the associations between them. It can bid a plan from which the products can be procured, and the system developed the work together to implement the overall coordination.

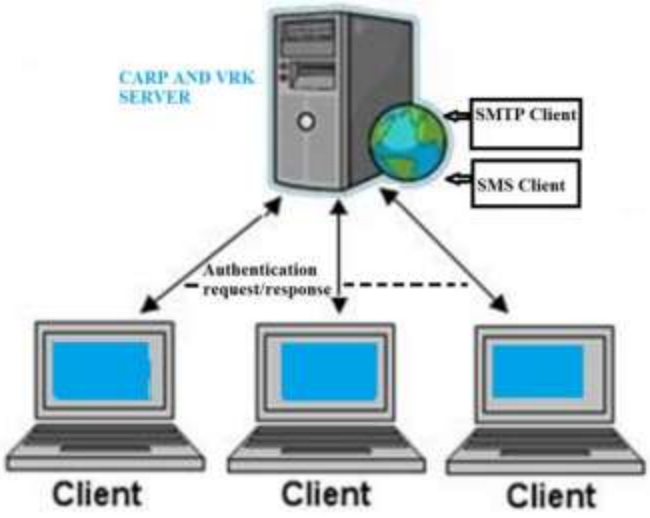

Figure 2: System Architecture

The system architecture comprised of 5 major blocks in the user the server SMTP client and the SMS client, and the Application for logging. The SMS client and email clients is connected server to the clients for communicating the LTP and OTP to the clients. The total flow and proposed system architecture is mentioned [13]. .In our proposed system it is based on partially observable attacker model. In we will propose an improved color pass shoulder surfing resistant password scheme [14]. use colors.

4. Proposed Scheme

It take simple and convenient shoulder surfing resistant graphical password system based on texts and colors. The 64 characters is used in this scheme which consist 26 upper case letters, 26 lower case letters, 10 decimal digits, and symbols.. These schemes take two phases the

registration phase and the login phase described as in the following [15].

A. Registration phase

The user has to enter his personal details contact details and account details as his pass color from 8 colors given by the system. In account details user will enter the 10 digit card number. The account number and textual password length automatically generated by the system. Textual password is sent to users to sms. The user has to enter an e-mail address for re-enabling his disabled account [16].

B. Login phase

The user requests for login the system and the system displays a circle which is divided into 8 equal sizes of sectors. Each sector is different color and each sector is recognized by the color of its the yellow sector is the sector of yellow is stating 64 characters are placed randomly in these sectors. These 64 characters is rotated simultaneously into adjacent sector either clockwise and anticlockwise by clicking the "clockwise" button or "Anticlockwise" button once respectively. The login screen of the proposed scheme is applied [17].

Fig.3: An example of the login page

C. Algorithms

Bresenham's Line Drawing Algorithm

This algorithm is use to divide into 8 sectors to place the characters in every sector at one line.

1. Read the line end points(x1,y1) and (x2,y2) such that they

are not equal. If they equal then plot that point and exit.

2. dx=|x2-x1| and dy=|y2-y1|

3. [Initialize starting point]

x=x1

y=y1

4. e=2*dy-dx

5. i=1[Initialize counter]

6. Plot(x , y)

7. while(e>=0)

{

y=y+1

e=e-2*dx

}

x=x+1

e=e+2*dy

8. i=i+1

9. if(i<=dx) then go to step 6

10. Stop.

The login system is in stuffiest for three times account is disabled and the system will send the email to the user's registered e-mail address and secret link that can be used by the legitimate user to renewable his disabled account [18].

C. Virtual Random Keyboard (VRK)

Virtual Random Keyboard is number of securing the login systems from shoulder surfing attacks. The virtual random keyboard VRK is a Virtual On-screen Keyboard having all numbers and characters displayed on it but with an innovative model to shuffle the characters on the keyboard buttons in random pattern so as to distract the shoulder [19] surfing attacker is hiding the characters being pressed. Working of VRK is as explained below:

1) Initialize the virtual keyboard to QWERTY keypad.

2) Accept the first character as numeric character considering it as length of password only,

3) On first character click, call random function over 26 characters and 10 digits for shuffling of the keyboard layout.

4) Display the randomized characters on the virtual keyboard keys.

5) For every consecutive click, call random function till submit buttons clicked.

6) Store the entered characters as user entered password and pass it for authentication using username and password.

E. OTP LTP Authentication (OLA)

Number of banking applications for security user and transactions make use of One Time Passwords (OTPs) to verify the transacting user and security valid user doing transaction. But the traditional model is hacked if the users SIM card is hacked and the OTP SMSs are retrieved by the attackers in between the OTP is eavesdropped [20]. secure the OTP system an additional process of involving the Long Term Passwords for authenticating the users have is proposed in this system making the attacker task number of difficult as compared to present OTP . The OTP is entered as it is instead the OTP is arithmetically computed with LTP previously sent over mail id and the new number obtained by post result the arithmetic operation is used as a secure pin to validate the authorized user.

The generation of LTP and OTP is as mentioned below:

1) The OTP and LTP generation functions is provided with

length of OTP and LTP to be generated.

2) The random function is take limits for each

digit from 0 to 9.

3) The random function is called for n number of times

where n is length of OTP.

4) The Once n number of random numbers is created the

numbers of concatenated to form a 4 digit OTP.

5) The LTP is generated using the same method and

Find as mail to the corresponding user mail id.

D. ONE-WAY-HASH-FUNCTION (HMAC)

HMAC represents the Hash Message Authentication Code. HMAC is number of function that it condenses a variable length message M to a fixed sized message by using the secret key K through many compression function. Hash functions is generally faster. Hash includes a key with message. Original proposal of a hash function is, Keyed Hash = Hash (Key | Message).

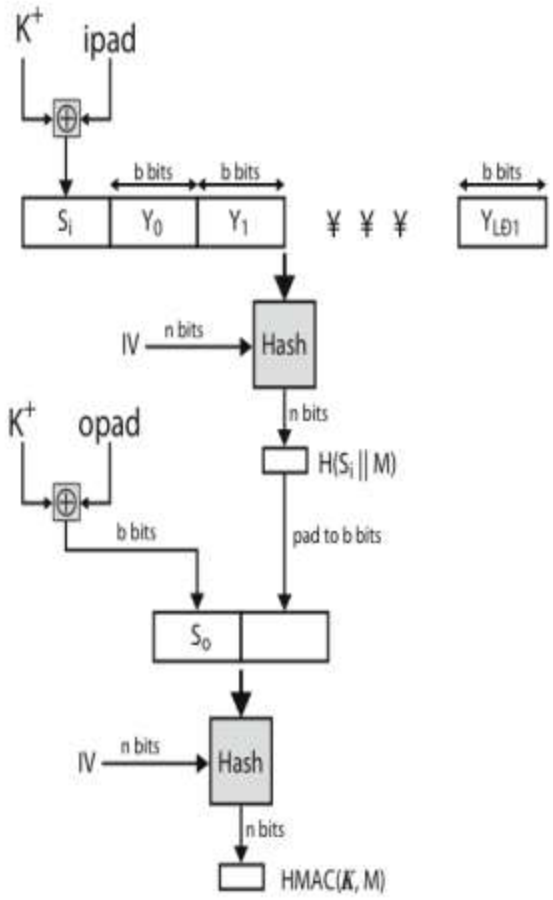

Fig4. HMAC overview

HMACK = Hash[(K+ XOR opad) || Hash[(K+ XOR ipad)||M)]]

where K+is the key padded out to size and ipad, opad are the specified padding constants overhead of HMAC relates to that of the primary hash algorithm attacking HMAC requires either the brute force attack on key used and birthday attack.

5. CONCLUSION

Passwords approaches many useful properties as well as widespread number of deployment

consequently we can expect their use for the foreseeable standard methods for password input is subject to a variety of attacks based on observation from casual eavesdropping to more exotic methods. The use of VRK, OTP and LTP and newly proposed Graphical password models highly secure the user authentication model and elemanete small users from accessing the system without security bypass. . The HMAC algorithm is used to provided secure PIN after the logon procedure human shoulder surfing attack is prevented and a secure transaction many mobile App and Server is established by using session Key Models. The user can easily and efficiently to login the scheme without using any physical keyboard. Finally we have analyzed resistances of proposed scheme to shoulder surfing and accidental login.

6. FUTURE WORK

The password is extracting some additional entropy bits from the gaze path that the user to entering the password. A new user is use completely different well times. As result stealing the user's password is insufficient for logging in and the attacker our results showed that the trigger-based model is considerably higher error rates due to eye-hand coordination, it is modify accounted for algorithmically by examining the historical gaze pattern and correlating it with trigger method..

7. REFERENCES

[1] S. Sood, A. Sarje, and K. Singh, "Cryptanalysis of password authentication schemes: Current status and key issues," in Methods and Models in Computer Science, 2009. ICM2CS 2009. Proceeding of International Conference on, Dec 2009, pp. 1–7.

[2] Duchowski, A. T., Eye Tracking Methodology: Theory and Practice: Springer. 227 pp. 2003.

[3] Golle, P. and D. Wagner, Cryptanalysis of a Cognitive Authentication Scheme, International Association for Cryptologic Research, July 31 2006.

[4] H. Zhao and X. Li, ―S3PAS: A Scalable ShoulderSurfing Resistant Textual-Graphical Password Authentication Scheme‖, in 21st International Conference on Advanced Information Networking and Applications Workshops, vol.2. Canada, 2007, pp. 467- 472.

[5] R. Biddle, S. Chiasson, and P. C. van Oorschot, Graphical passwords: Learning from the first twelve years,‖ ACM Comput. Surveys, vol. 44, no. 4, 2012.

[6] P. C. van Oorschot and J. Thorpe, Exploiting predictability in clickbased graphical passwords,‖ J. Comput. Security, vol. 19, no. 4, pp. 669–702, 2011

[7] L. Sobrado and J. C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[8] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in CRYPTO, pp. 104–113, 1999.

[9] R. Biddle, S. Chiasson, and P. C. van Oorschot, Graphical passwords: Learning from the first twelve years,‖ ACM Comput. Surveys, vol. 44, no. 4, 2012.

[10] S. Chiasson, P. C. van Oorschot, and R. Biddle, Graphical password authentication using cued click points,‖ in Proc. ESORICS, 2007, pp. 359–374.

[11] Roth, V., K. Richter, and R. Freidinger. A PIN-Entry Method Resilient Against Shoulder Surfing. In Proceedings of CCS: Conference on Computer and Communications Security. Washington DC, USA: ACM Press. pp. 236-45, 2004.

[12] Phen-Lan Lin, Li-Tung Weng and Po-Whei Huang, Graphical passwords using images with random tracks of geometric shapes,‖ 2008 Congress on Images and
Signal Processing. 2008.

[13] K. Renaud and E. Smith. Jiminy: ―Helping user to remember their passwords‖. Technical report, School of Computing, Univ. of South Africa, 2001.

[14] T.Perkovic,M.˝Cagalj, and N.Saxena, "Shouldr surfing safe login in a partially observableattacker model," in Sion, R.(eds.) FC 2010. LNCS,pp .351–358, 2013

[15]M. Sreelatha, M. Shashi, M. Anirudh, Md. Sultan Ahamer, and V. Manoj Kumar, "Authentication schemes for session passwords using color and images," International Journal of Network Security & Its Applications, vol. 3, no. 3, May 2011.

[16] M. K. Rao and S. Yalamanchili. "Novel shoulder-surfing resistant authentication schemes using text-graphical passwords," International Journal of Information & Network Security, vol. 1, no. 3, pp. 163-170, Aug. 2012 .

[17]Yi-Lun Chen, Wei-Chi Ku, Yu-Chang Yeh, and Dun-Min Liao, "A Simple Text-Based, Shoulder Surfing Resistant Graphical Password Scheme", IEEE 2nd International Symposium on Next-Generation Electronics (ISNE), Feb.2013.

[18] L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudorandom number generator," SIAM Journal on Computing, vol. 15, pp.

364–383, may 1996.

[19] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in CRYPTO, pp. 104–113, 1999.

[20] L. Zhuang, F. Zhou, and J. D. Tygar, "Keyboard acoustic emanations revisited," in ACM Conference on Computer and Communications
Security, pp. 373–382,

ABOUT AUTHORS:

K.Tholi Sandhya is currently pursuing her **MCA** in MCA Department, **St. Ann's college of Engineering & Technology, Chirala** , A.P. She received her Bachelor of Science from **ANU.**

P.S.NAVEEN KUMAR received his M.Tech. (CSE) from jntu Kakinada. Presently he is working as an Assistant Professor in MCA Department, **St.Ann's College Of Engineering & Technology , Chirala.** His research includes networking and data mining.