International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 12, December-2015

Design and Implementation of Session Authentication against Shoulder Surfing Attack

Miss. Pranjali Waghmare
Dept of Computer Science and Engineering
GHRAET, Nagpur, India

Prof. Sonali Bodkhe
Dept of Computer Science and Engineering
GHRAET, Nagpur, India

***Abstract*- Very well known traditional method of authentication is alphanumeric password i.e. text based password. a Text based passwords are vulnerable to various attacks such as dictionary attack, social engineering, etc. To resist such attacks graphical passwords were introduced. Graphical passwords were used to increase the memorability of user but this technique undergoes several attacks such as shoulder surfing attack. To deal with this problem, we proposed session password authentication technique. In this technique the password changes for each login. So this scheme may help to reduce the shoulder surfing attack.**

Keyword: Graphical passwords, Session authentication, Shoulder surfing attack.

1. INTRODUCTION

Security of the computer system is a first priority to any user. Authentication of a user is proper way to provide better security. Most common method was textual password authentication. That was a simple and easy technique of authentication. But it undergoes various attacks like social engineering, dictionary attack, etc. To resist these attack, graphical password authentication technique was introduced. Human psychology states that, human mind can memorize picture better than text. So this scheme was useful to memorize a password. But it was susceptible to the shoulder surfing attack. To deal with this attack we implement session password authentication, which provide better security to user.

Session password authentication technique is based on chess game. Here we used some chess rules for creation of password. Most people know chess game and its rule, so this technique helps to improve the recall ability of password. Here we used movement of three characters i.e. Rook (Elephant), Bishop (Camel), and Knight (Horse) to implement the session password. This session password always generate new password for each login. So it is help to reduce the shoulder surfing attack.

2. RELATED WORK

Security of data is basic need for computer system. Alpha-numeric passwords were well known and old authentication technique. Most users were very familiar with that password system as this was easy for use, but it undergoes various attacks. Such as, dictionary attack, shoulders surfing attack, etc. As textual authentication undergoes many attacks so to overcome these attacks graphical authentication technique were introduced. Many graphical authentication based techniques were introduced by the researchers. In 1996, blonder [1] presented graphical password concept. In which user had to enter some points on image in a sequence. R. Dhamija and A. Perrig [2] proposed a déjà vu authentication technique in which system provided password images as well as some decoy images. User had to choose the correct image for successful authentication. But this technique undergoes shoulder surfing attack. Passfaces [3] is authentication technique in which user had to select four images in sequence and should remember it. Same process was repeated for four times. It was vulnerable to shoulder surfing attack. Wiedenbeck et. al. [4],[5],[6] proposed passpoint authentication scheme. In which user had to select some points on the image and User should remember points as well as sequence of clicks. It was quiet hard for user to remember. Jermyn et. al. [7] proposed DAS authentication system for PDA. In this technique user had to draw a particular sequence by mouse. This was very difficult to the user to remember sequence. Syukri [8] designed Signature technique. User had to enter signature as input using mouse. But everyone was not familiar with drawing signature with mouse so this system failed. S. Chiasson proposed [9] concepts in which images were provided to user. User has to select several points on the image. Persuasive cued click point [10], [11], [12] was concept which was similar to cued click point. User had to select five different images in a sequence and five grids from each image. But this system undergoes shoulder surfing attack. Graphical authentication systems were easy to used but there were many drawbacks which give high failure rate so to overcome these drawbacks and to provide better security to user, session password authentication technique was introduced. Session authentication [13], [14] was a technique where password changes during each login. This was based on textual authentication. This system was also called as pair base authentication. In Hybrid textual authentication eight colors were provided to user. User should give numbers to color and should remember it. User had to enter correct sequence of colors. Pass pair system does not provide pass pair for identical letters like “ss”. Hybrid textual technique could not be applicable for colorblind people.

3. SESSION PASSWORD AUTHENTICATION

In this section we are discussing process of Session authentication. In this technique, user has to provide their password by conventional method. This password is also known as original password (P). In this

technique we used virtual keyboard. Virtual keyboard contain only upper case alphabets. While entering password, user can also enter password in lower case mode. It will reduce the complexity of password. In this scheme, we combined chess characters and implement three different methods i.e.

- Bishop-Rook movement,
- Knight Movement, and
- Knight-Bishop movement.

This authentication system has three phases, first is Registration, second is Login, and third is Verification phase. In registration phase user has to provide username, original password and any one authentication technique from above. In login phase, user provides username. For entering password user has to used the technique which was chosen at the time of registration. In verification phase, system will verify the password according to technique. The alphabet use in propose scheme contain 36 characters, including 26 upper case letters and 0-9 number digits. At the time of generation of Session password, we split original password (P) in pass pairs. i.e. P_1P_2, P_3P_4….. $P_{n-1}P_n$.

Following are some rules, that user should remember for successful authentication.

If original password contain identical symbols near to each other i.e. SS, then use following rule.

- Upper Right next element using Bishop move

For example, we consider PRIYAA1 as our original password. So the pass pairs for this password are PR, IY, AA, 1P. Here 'AA' is pair which has consecutive identical letters. we will consider upper right next element using Bishop Movement for generating session password. Here length of password is 7, means our password has odd length. In that case, we combine last letter i.e. 1 and first letter i.e. P with each other and form pair as 1P for generating session password. These two rules user must remember in registration process as well as in login process.

3.1 Notation

Following notations are use for analysis and discussion, right through this paper.

- K – Set of characters on grid
- |K| - Total number of characters on Grid
- |P| – Original password
- |L| - Length of session password.
- |S|- Set of rules use in this technique.

3.2 Bishop-Rook Rule:

In this method, we used Bishop and Rook movement for creation of session password. In chess game, Bishop can moves any number of squares in diagonal direction and Rook can moves any number of squares in vertical or horizontal direction. Here we intersect both the pass pairs using Bishop and Rook movement with each other. Intersection will form Common Square which is our first Session password. Likewise same process will be repeated for remaining pairs. As Rook can move in two directions i.e. Vertical and Horizontal. So for ease of use, user has to choose one of following rule to create session password at the time of registration.

a) Bishop - Rook (Vertical)
b) Bishop - Rook (Horizontal)
c) Rook (Vertical) – Bishop
d) Rook (Horizontal) – Bishop

a) *Bishop - Rook (Vertical):*

If we consider original password as "SAKSHI", Pass pairs of original passwords are SA, KS, and HI. For first pair SA, 'S' used Bishop Movement and 'A' used Rook movement. Intersection of both letters formed first character of session password i.e. 4. Session password for this rule is '403'.Black circle represents original and Red circle represents Session password.

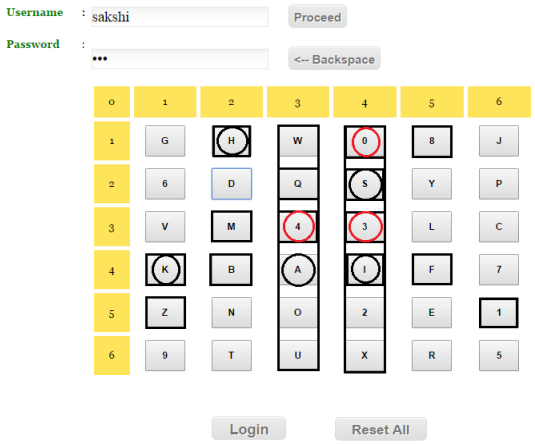

Fig 3.2(a): Session password for Bishop and Rook (V) Rule.

New session password for this technique is "403". Generation of session password has been shown in above figure 3.2(a).

This same concept is applicable to the remaining methods in Bishop-Rook rule. Snapshots for these methods are shown in following figures i.e. fig 3.2 (b), fig 3.2(c), Fig 3.2(d).

b) *Bishop - Rook (Horizontal):*

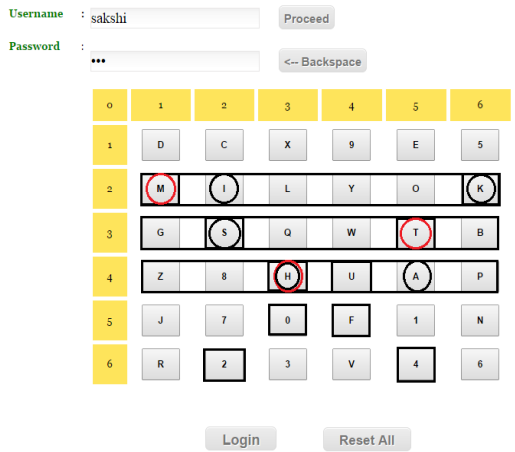

Fig 3.2(b): Session password for Bishop and Rook (H).

c) *Rook (Vertical) - Bishop:*

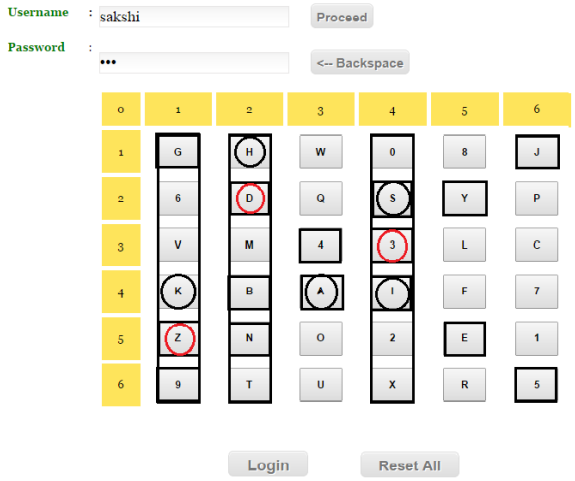

Fig 3.2(c): Session Password for rule Rook (V) and Bishop.

d) *Rook (Horizontal) - Bishop:*

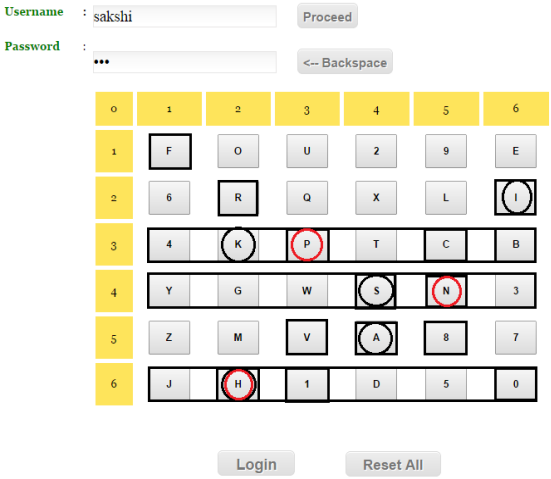

Fig 3.2(d): Session password for Rook (H) and Bishop Rule.

3.3 Knight Rule

Knight rule is simple and easy to use. Most people know movement of Knight in chess game. In chess, knight moves in eight possible squares. Same rule we apply here for creating new password. If we considered original password as "JENY", Length of original password is 4. Session password will have same length i.e. 4. Here we apply knight rule to single character. So both passwords are of same length.

For example, according to knight rule there are 8 possible squares to choose as password user can choose any one from eight possible squares. But as shown in following figure 3.3 (a) in case of first letter 'J' and third letter 'N' both are situated at two different extreme corners. So both letters have two possible squares for selection. For letter 'J' user can select either M or V. we select letter 'V' as first session password. For letter 'N' user can choose X or K. we select 'K'. Letter 'E' is in center so it has total eight possible squares to choose as password. i.e. V,3,Q,6,M,5,H, and T. here we select 'Q' and letter 'Y' has three possible squares i.e. D, S, K. from which we select D. so the password for Knight rule is "VQKD".

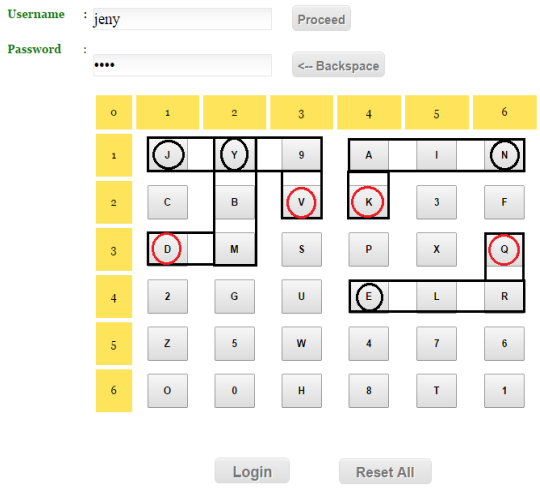

Fig 3.3(a): Session password using Knight

3.4 Knight – Rook Rule

This scheme uses two chess characters i.e. Knight and Rook. According to chess game Knight moves in eight possible squares and Rook moves in two directions i.e. Vertical and Horizontal direction. Here first letter of original password used knight movement and second letter used Rook movement. In Knight – Rook rule there is no restriction for use of vertical or horizontal direction of rook movement. Here rook rule varies according to user's choice.

For example, if we consider "SAKSHI" as original password. Pass pairs for original password SAKSHI are SA, KS, and HI. In case of SA pass pair 'S' uses Knight Rule and 'A' uses Rook rule in horizontal direction. Intersection of both letters formed common square i.e. 'Y'. For next pair "KS", Common square form by both letters is 'U'. Last pass pair is "HI". Intersections of both pass pair formed Common Square i.e. '7'. So session password using knight – Rook rule is "YU7".

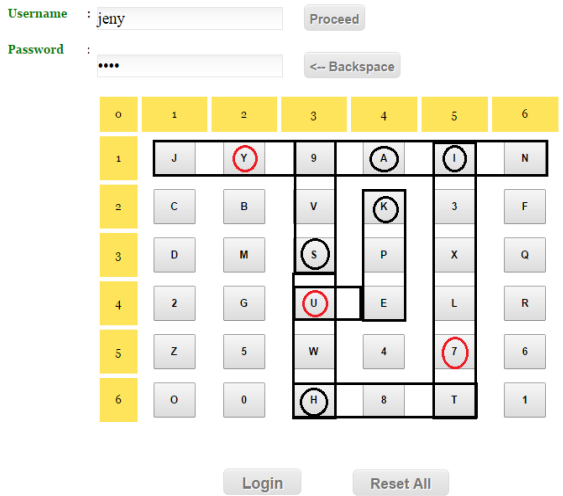

Fig 3.4: Session password for Knight Rook

4. ANALYSIS AND DISCUSSION

Session authentication is a concept works on session. For each session different password will be generated. Generation of new password each time is strength of this technique. This technique reduces many attacks such as, dictionary attack, brute force attack, random click attack, shoulder surfing attack, etc.

Complexity: Complexity of this technique is depends on original password. All clicks done by the user are related to original password. So the complexity of original password of |L| will be $|K|^{|L|}$.

Shoulder surfing attack: A person or a device who detect password by observing the keystroke enter by user is called shoulder surfing attack. Interface is changing in each session will reduce the shoulder attack possibility. All six Authentication techniques provide security against Shoulder Surfing Attack. No other different mapping is required to calculate shoulder Surfing attack.

Guessing: Guessing attack is not possible in this technique. Each time new password will be generated, so no one can guess the password. Which mean Guessing attack is reduces by this technique. Possible combinations for this technique are $|S|\times|K|^{|L|}$.

Dictionary attack: In this type of attack, attackers use dictionary words one by one to authenticate. Original password is hidden in this technique so, this attack is not possible. This attack is also resist by session authentication.

Brute force attack: Brute force attack can also be resist by session authentication technique, as it generate new password for each login.

Random Click Attack: Random click attack can be occurred by clicking randomly. But this attack also not possible in this technique, because each login interface will be different as a result password is also changed. Success probability of Random click attack is given as follows:

$$P(S) = \frac{|L|}{|S|\times|K|^{|P|}} = |L|\times|S|^{-1}\times|K|^{-|P|}$$

Where $|L| \geq [|P| / 2]$

Success probability of random click attack is as follows:

If |S| = 6, |K| = 36, |P| = 8,

Then $P(S) = 5.91\times10^{-14}\ |L|$

This is very negligible value. As we increase the value of |P| then success Probability will decreases for random click attack It means that random click attack is not possible in this scheme

5. COMPARISON ANALYSIS

Techniques	Conventional	Graphical	Session
Usability	Very High	High	Moderate
Flexibility	Moderate	High	Moderate
Features	easy to memorize	Easy to remember	Hard to guess
Resist attacks	-	Dictionary Attack, Brute force attack, etc	Shoulder Surfing attack, dictionary attack, spyware, bruteforce,etc.
Memorability	Less	High	High

6. CONCLUSION:

This authentication technique is design to resist shoulder surfing attack. along with shoulder surfing attack it can resist to brute force attack, dictionary attack, man in middle attack, random click attack, etc. as this technique is based on chess rule it is easy to user to memorize all rules of this technique. It will increase security as well as it provides better usability to user. To find the minimum and maximum time required to use each rule and use of special symbols in virtual keyboard is my future work.

REFERENCES

[1] Blonder, G.E. Graphical Passwords. United States Patent 5,559,961, 1996

[2] A. Perrig, and R. Dhamija "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.

[3] Real User Corporation: Passfaces. www.passfaces.com

[4] J. Waters, S. Wiedenbeck, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in Human- ComputerInteraction International (HCII 2005). Las Vegas, NV, 2005

[5] J. C. Birget, S. Wiedenbeck, J. Waters, A. Brodskiy,and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in Symposium on Usable Privacy and Security. Carnegie Mellon University, Pittsburgh, 2005.

[6] A. Brodskiy, S. Wiedenbeck, J. Waters, J. C. Birget, and N. Memon,"PassPoints: Design and longitudinal evaluation of a Graphical password system," International Journal of Human Computer Studies.

[7] A. Mayer, I. Jermyn, F. Monrose, M. K. Reiter, and A.D. Rubin in Proceeding of Design and Analysis of Graphical password. In the 8th USENIX Security Symposium, 1999.

[8] M. Mambo, F. Syukri, E. Okamoto and "A User Identification System Using Written with Mouse," in Australian Conference on Information Security and Privacy : Springer-Verlag Notes in Computer Science (1438), 1998, pp.403- 441.

[9] R. Biddle, S. Chiasson, P. van Oorschot, And "Graphical Password Authen -tication Using Cued Click Points ," Proc. European Symp. Research in Computer Security , pp. 359-374, Sept. 2007

[10] A. Forget, S. Chiasson, R. Biddle, and P. C. van Oorschot. Influencing users Towards better passwords: Persuasive Cued Click-Points. In BCS-HCI '08: Proceedings of the 22nd British HCI Group Annual Conference on HCI. British Computer Society, Sept 2008.

[11] E. Stobert, S. Chiasson, A. Forget, 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.
[12] P. C. van Oorschot, S. Chiasson, E. Stobert, A. Forget, R. Biddle, and "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism",IEEE transactions on dependable and secure computing, vol. 9, no. 2, march/april 2012.
[13] M. Shashi, M. Sreelatha, M. Anirudh, MD. Sultan Ahmar and V. Manoj Kumar,"Authentication Schemes for session Passwords using Color and Images". International Journal of Network Security and its Application (IJNSA), Vol.3, No.3, May 2011.
[14] D. S. Devi, M. T. Selvi, T. Sowmiya, M.J. Pavithra, J. J. Emilyn"Generating Session Password using Text and Color to Prevent Shoulder Surfing" International conference on modeling optimization and computing,2012.