International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Preventing A Shoulder Surfing Attack Using Graphical Authentication System

[1](Bindhu K G, Chaithra C, Lakshmi Kavya P, Namratha D P), [2]Manu Y M

[1](UG students,Dept. of CSE, BGSIT, VTU, Karnataka, India)
[2](Assistant prof.,Dept. of CSE, BGSIT, VTU, Karnataka, India)

Abstract- *Authentication based on passwords is used widely in applications for computer security and privacy. Still, our actions such as choosing bad passwords and inputting them in an insecure way are known as "the weakest link" in the authentication ring. Rather than arbitrary alphanumeric strings, users tend to sets his passwords either short or meaningful for easy remembrance. This evolution brings great assurance but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' information. To overcome this problem, we proposed a novel authentication system comprising PassMatrix, based on graphical passwords to resist shoulder surfing attacks. Valid login indicator and circulative horizontal and vertical bars with one time covering the entire scope of pass-images, this matrix doesn't give any hint for attackers to trace out the password even if they use multiple camera-based attacks. To evaluate its memorability and usability, we also implemented a PassMatrix prototype on Android and carried out real user experiments. From the experimental result, the proposed system achieves better security to shoulder surfing attacks.*

Key Words—Graphical Passwords, PassMatrix, Shoulder Surfing Attack.

1.Introduction

Textualpasswords have been the most largely used authentication method for ages. Consisting of numericals and letters of both upper- and lower-case, textual passwords are considered strong enough to resist against brute force attacks. Still, a strong textual password is hard to remember .Hence, users tend to choose passwords that are either from the dictionary or short , rather than random alphanumeric strings. Even worse, it is not a rare case that users may use only one username and password for multiple accounts . According to an article in Computer world, a security team at a large company ran a network password cracker and surprisingly cracked approximately 80% of the employees' passwords within 30 seconds. Textual passwords are often insecure due to the difficulty of maintaining strong ones. Various graphical password authentication schemes , were developed to address the problems and weaknesses associated with textual passwords. Based on some studies such as those in humans have a better ability to memorize images with long-term memory (LTM) than verbal representations. Image-based passwords were proved to be easier to recollect in several user studies. As a result, users can set up a complex authentication password and are capable of recollecting it after a long time even if memory is not activated periodically.However, most of these image-based passwords are vulnerable to shoulder surfing attacks (SSAs). This type of attack either uses direct observation, such as watching over someone's shoulder or applies video capturing techniques to get passwords, PINs, or other sensitive personal information [13], [14], [15]. The human actions such as choosing bad passwords for new accounts and inputting passwords in an insecure way for later logins are regarded as the weakest link in the authentication chain [16]. Therefore, an authentication scheme should be designed to overcome these vulnerabilities. In this paper, we present a secure graphical authentication system named PassMatrix that protects users from becoming victims of shoulder surfing attacks when inputting passwords in public through the usage of one-time login indicators. A login indicator is randomly generated for each pass-image and will be useless after the session terminates. The login indicator provides better security against shoulder surfing attacks, since users use a dynamic pointer to point out the position of their passwords rather than clicking on the password object directly.

1.1.PASSMATRIX

PassMatrix is to overcome the following:
(1) the security weakness of the old
PIN method
(2) the easiness of finding passwords by
observers in public
(3) the compatibility issues for the

devices, we introduced a graphical authentication system called PassMatrix.
In PassMatrix, a password consists of
only one pass-square per pass-image to a sequence of n images. The number of images (i.e., n) is user-defined.
In PassMatrix, users chooses one square per image in a sequence of n images rather than n squares for one image as that in the PassPoints scheme. Based on the Cued Click Points (CCP) proposed by Chiasson et al the CCP method posses a good job in helping users recollect and easy to remember their passwords. If the user clicks on an incorrect region within the image, a different image will be shown to give the user a warning feedback. Figure 5 explains the proposed model, in which the
first pass-square is placed at (4, 8) in the first image, the second pass-square is on the top of the smoke in the second image at (7, 2), and the last pass-square is at (7, 10) in the third image.

Fig. 5. A password contains three images (n=3) with a pass square ineach. The pass squares are shown as the orange-filled area in each image.

2. System Architecture

PassMatrix is comprised of the following components (see
Figure 6):
_ Image Discretization Module
_ Horizontal and Vertical Axis Control Module
_Login Indicator generator Module
_ Communication Module
_ Password Verification Module
_Database

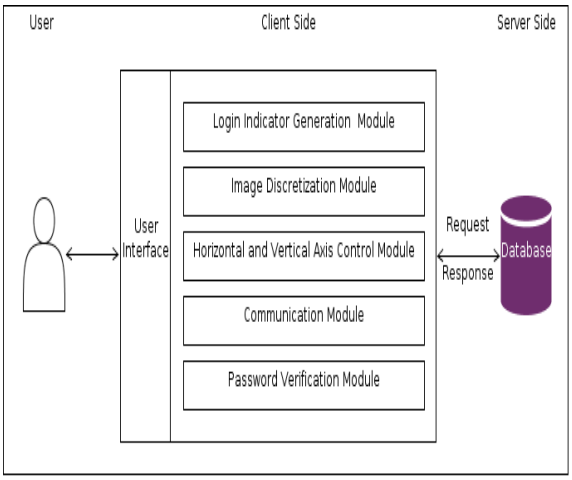

Fig. 6. Overview of the PassMatrix system.

Image Discretization Module. users would choose one square as the pass-square. **In which**This module divides each image into squares,

Login Indicator Generator Module. This module produces a login indicator consisting of several distinguishable characters (such as alphabets and numbers) or visual materials (such as colors and icons) for users during the authentication phase.

Horizontal and Vertical Axis Control Module. There are two scroll bars: a horizontal bar with a sequence of letters and a vertical bar with a sequence of numbers.
T his control module provides **drag** and **fling** functions for users to control both bars.

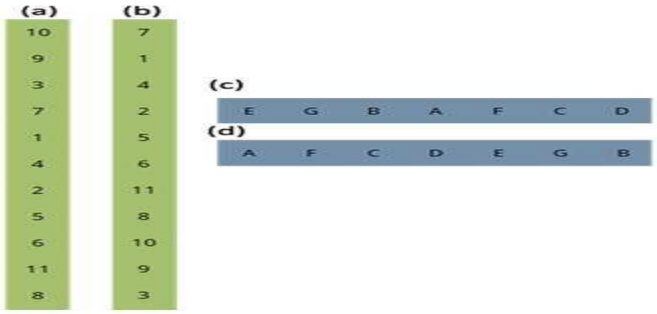

Fig. 8. Horizontal scroll bar (on the right/blue) and vertical bar (on the left/green).

Communication Module. This module is in charge of all the information transmitted between the client devices and the authentication server.

Password Verification Module. This module verifies the user password during the authentication phase.

Database. The database server contains several tables that store user accounts, passwords (ID numbers of passimages and the positions of pass-squares), and the time duration each user spent on both registration phase and login phase. PassMatrix has all the required privileges to perform operations like insert, modify, delete and search.
PassMatrix's authentication includes a registration phase and an authentication phase as described below:
4.2.1 Registration phase

Figure 9 is the flowchart describes the registration phase. At this stage, the user establishes an account which contains a username and a password. The password contains only one pass-square per image for a sequence of n images.

The number of images (i.e., n) is decided by the user after considering the trade-off between security and usability of the system . The only use of the username is to give the user an imagination of having a personal account.The username can be omitted if PassMatrix is implement to authentication systems like screen lock. The user can either choose images from a provided list or upload images from their device as pass-images. Then the user will take a passsquare for each selected pass-image from the grid, which was divided by the image discretization module. The user repeats this process until the password is set. Authentication phase is shown in the below figure.

The user uses his/her username, password and login indicators to log into PassMatrix. The following describes all the steps in detail:

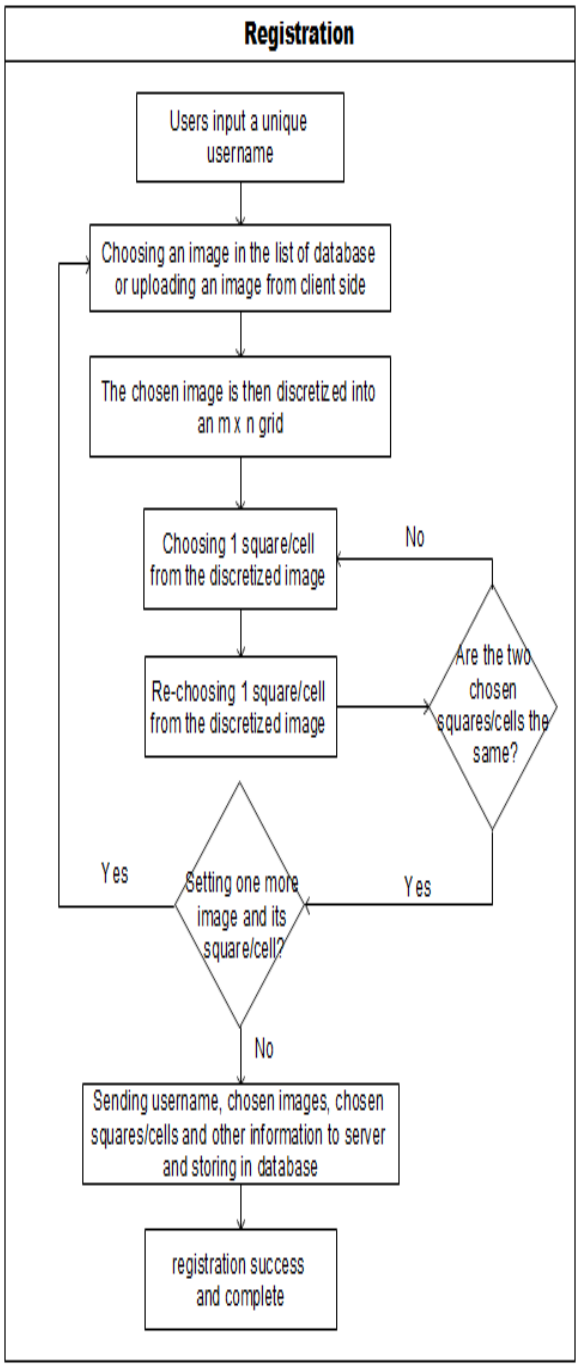

Fig. 9. The flowchart of registration phase in PassMatrix.

1) The user inputs his/her username which was created
in the registration phase.
2) A new indicator comprised of a letter and a number is created by the login indicator generator module.
The indicator will be shown when the user uses IEEE Transactions on Dependable and Secure Computing (Volume:PP , MARCH 2016) his/her hand to form a circle and then touch the screen. In this case, the indicator is conveyed to the user by visual feedback. The indicator can also be delivered through a predefined image or by audio feedback that we have mentioned in the previous section.
3) Next, the first pass-image will be shown on the display, with a horizontal bar and a vertical bar on its top and left respectively. To respond to the challenge, the user flings or drags the bars to align the pre-selected pass-square of the image with the login

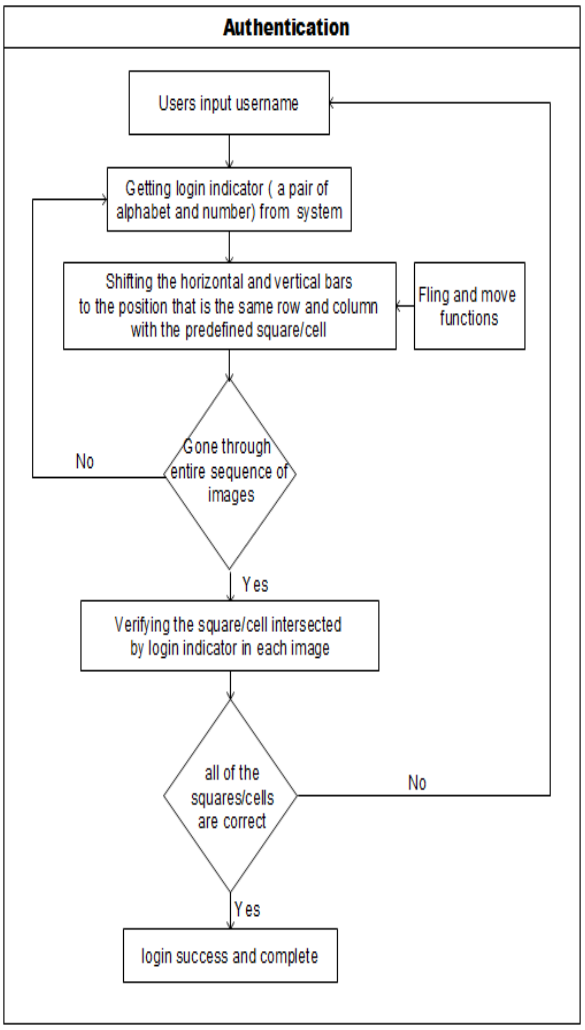

Fig. 10. The flowchart of authentication phase in PassMatrix.

Indicator. For example, if the indicator is (E,11) and the pass-square is at (5, 7) in the grid of the image, the user shifts the character ”E” to the 5th column on the horizontal bar and ”11” to the 7th row on the vertical bar (see Figure 12).4) Repeat step 2 and step 3 for each pre-selected passimage.
5) The communication module gets user account information from the server through HttpRequest POST method.
6) Finally, for each image, the password verification module verifies the alignment between the passsquare and the login indicator. Only if all the alignments
are correct in all images, the user is allowed to log into PassMatrix.

3.Implementation

The PassMatrix prototype was built using Android SCX SDK 2.3.3 which was the mainstream version of the distribution in 2012 . After connecting to the Internet, users can register an user account, log in to their account few times in practice mode, and then log in for the experiment with a client's device (see Figure11(a)).We used XML in the client side to build the user interface and used JAVA and Android API to implement functions, which includes username checking, pass images listing, image discretization, pass-squares selection,login indicator delivery, and the horizontal and vertical bars circulation.We used PHP and MySQL on the server side of implementation, to store and also fetch registered accounts to/from the database to handle the password verification.
In our proposed system we mentioned that users can import their own images, we have used a list of 24 fixed test images in our experiment.

4.Experimental Results

We have analyzed the collected data from our experiments to evaluate the effectiveness of the proposed system.The results are given in two perspectives: accuracy and usability.In the practice phase of the first session, participants practiced the login process for 4 times(average) ranging from 1 to 14 (excluding one outlier) and then moved onto the authentication (login) phase. As we defined in the previous section, participants can keep trying to log in to their account eventhough they have failed six times.A successful attempt means that a user, in less than or equal to six tries, is able to pass the authentication with a correct password. If all the six attempts are failed, then it will be marked as failure. Below, we define two terms First Accuracy and Total Accuracy which are used in our experiment:

First Accuracy =Successful attempts in first Try Total attempts
(1) IEEE Transactions on Dependable and Secure Computing (Volume:PP , MARCH 2016)
Total Accuracy =Successful attempts
Total attempts

4.1. Usability

We counted the number of shifts and the elapsed time per pass-image to measure the usability of PassMatrix in practice in the experiment.

4.2. SECURITY ANALYSIS

In this section we examine the security of the proposed authentication system against three types of attacks: random guess attack, shoulder surfing attack, and smudge attack.

4.2.1. Random Guess Attack

To perform a random guess attack, the attacker randomly tries each square as a pass-square for each passimage
until a successful login occurs. To quantify
the security of PassMatrix against random guess attacks, we define the entropy of a password space as in equation
3.Entropy = log2((Dx _ Dy)i)n (3)

4.2.2. Shoulder Surfing Attack

Although we know the fact that shoulder surfing has been a real threat to authentication systems with either textual or graphical passwords,a number of novel authentication schemes were proposed to protect systems from this attack. Unfortunately, most of them were unsuccessful to identify threat if the shoulder-surfing attack is camera-based. For instance,some schemes such as PIN-entry method [34] and spyresistant
keyboard [19] were designed on the basis of short-term memory. Camera-based shoulder surfing attacks are used to crack the passwords of these schemes.

4.2.3. Smudge Attack

A smudge attack is an implicit attack where attackers try to extract sensitive information from recent users' input by inspecting smudges present on touch screens. Since both the horizontal and vertical bars in PassMatrix are scrollable, shifting on any element within the bar can use the whole bar. Thus, users do not have to shift the bars by touching the login indicators. The smudge left by users may
be static, but it points to the habitual stretching range of the thumb or finger. The length of the smudge left on the screen does not provide any useful information since the login indicator is generated randomly for each pass-image and the permutations of elements on both bars are also randomly re-arranged in each pass-image and in login session. Hence we can conclude that the proposed PassMatrix is immune from smudge attacks.

5. Conclusion

With the increasing trend of web services and applications, users are able to access these applications anytime and anywhere using various devices. In order to protect users' digital datas,authentication is required every time they try to access their personal account. However, conducting the authentication and security process in public might result in potential shoulder surfing attacks because a complicated password can be cracked easily through shoulder surfing.
To overcome this problem, we proposed a shoulder surfing resistant authentication system based on graphical passwords, named PassMatrix. Using login indicator per image, users can point out the location of their pass-square without clicking or touching it, which is an action vulnerable to shoulder surfing attacks.
Because of the design of the horizontal and vertical bars which cover the entire pass-image, it does not provide any clue for attackers to narrow down the password space even if they have more than one login records of that account. Based on the experimental results and survey data, PassMatrix is considered a novel and easy-to-use graphical password authentication system, which can effectively alleviate shoulder-surfing attacks.

6. 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] S. Gurav, L. Gawade, P. Rane, and N. Khochare, "Graphical password authentication: Cloud securing scheme," in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014
International Conference on, Jan 2014, pp. 479–483.
[3] K. Gilhooly, "Biometrics: Getting back to business," Computerworld,May, vol. 9, 2005.
[4] R. Dhamija and A. Perrig, "Deja vu: A user study using images for authentication," in Proceedings of the 9th conference on USENIX Security Symposium-Volume 9. USENIX Association, 2000, pp. 4–4.
[5] "Realuser," http://www.realuser.com/.
[6] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proceedings of the 8th conference on USENIX Security Symposium-Volume 8. USENIX Association, 1999, pp. 1–1.
[7] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon,"Passpoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies,
vol. 63, no. 1-2, pp. 102–127, 2005.
[8] A. Paivio, T. Rogers, and P. Smythe, "Why are pictures easier to recall than words?" Psychonomic Science, 1968.
[9] D. Nelson, U. Reed, and J. Walling, "Picture superiority effect," Journal of Experimental Psychology: Human Learning and Memory, vol. 3, pp. 485–497, 1977.
[10] S. Brostoff and M. Sasse, "Are passfaces more usable than passwords?
a field trial investigation," PEOPLE AND COMPUTERS, pp. 405–424, 2000.
[11] A. De Angeli, M. Coutts, L. Coventry, G. Johnson, D. Cameron,and M. Fischer, "Vip: a visual approach to user authentication," in Proceedings of the Working Conference on Advanced Visual Interfaces.ACM, 2002, pp. 316–323.
[12] B. Ives, K. Walsh, and H. Schneider, "The domino effect of passwordreuse," Communications of the ACM, vol. 47, no. 4, pp. 75–78,2004.
[13] J. Long and K. Mitnick, No Tech Hacking: A Guide to Social Engineering,
Dumpster Diving, and Shoulder Surfing. Elsevier Science,
2011.
[14] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human adversaries are more powerful than expected," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 44, no. 6,pp. 716–727, June 2014.

[15] "Google glass snoopers can steal your passcode with a glance," http://www.wired.com/2014/06/google-glass-snoopers-cansteal- your-passcode-with-a-glance/.
[16] M. Sasse, S. Brostoff, and D. Weirich, "Transforming the weakestlinka human/computer interaction approach to usable and effective security," BT technology journal, vol. 19, no. 3, pp. 122–131,2001.
[17] "Mobile marketing statistics compilation,"http://www.smartinsights.com/mobile-marketing/mobilemarketing-analytics/mobile-marketing-statistics/.
[18] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in Proceedings of International conference on security and management, 2004.
[19] D. Tan, P. Keyani, and M. Czerwinski, "Spy-resistant keyboard: Towards more secure password entry on publicly observable touch screens," in Proceedings of OZCHI-Computer-Human Interaction
Special Interest Group (CHISIG) of Australia. Canberra, Australia:
ACM Press. Citeseer, 2005.
[20] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing shoulder-surfing by using gaze-based password entry," in Proceedings of the 3rd symposium on Usable privacy and security. ACM,
2007, pp. 13–19.

[21] A Shoulder Surfing Resistant Graphical Authentication System,Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng,2016

BIOGRAPHIES

BINDHU K G

UG STUDENTS, BGSIT

VTU

CHAITHRA C

UG STUDENTS, BGSIT

VTU

LAKSHMI KAVYA P

UG STUDENTS, BGSIT

VTU

NAMRATHA D P

UG STUDENTS, BGSIT

VTU

MANU Y M

ASST. PROF.,DEPT OF CSE BGSIT,

VTU