A Secure and Graphic Authentication Model to Detect and Prevent Shoulder Surfing Attacks

[1] Shiva Pampana, [2] Prof. Kasukurthi Venkata Rao
[1]Department of CST, A.U.College of Engineering (A), Andhra University, Visakhapatnam
[2]Department of CS&SE,A.U.College of Engineering (A) Andhra University, Visakhapatnam

Abstract: This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' credentials. To overcome this problem, we proposed a novel authentication system PassMatrix, based on graphical passwords to resist shoulder surfing attacks. Authentication based on passwords is used largely in applications for computer security and privacy. However, human actions such a choosing wrong passwords and inputted passwords in not secure way are regarded as "the weakest connection" in the authentication chain, Rather than arbitrary alphanumeric character, users tend to select a password either short or his name related for easy memorization. With web site applications and mobile phone apps charging up, peoples can get access to these types of application anytime, anywhere with multiple devices. This evolution brings good convenience but also improves the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect user's credentials. To overcome this problem, we proposed a novel authentication system Pass Matrix, based on graphical passwords to resist shoulder surfing attacks. Many authentication methods are presented, but users are familiar with textual password method. Textual password methods are vulnerable to shoulder surfing and key loggers. To overcome this problem many other authentication system like token based authentication, biometric based authentication systems, graphical password methods have been proposed. However biometric based authentication systems are costly and graphical password systems are secure and efficient.

Index Terms **- Graphical Passwords, Authentication, Shoulder Surfing Attack, PassMatrix.**

I. INTRODUCTION

Shoulder surfing technique is gathering information such as usernames and passwords by watching over a person's shoulder while he/she logs into the system, by helping attackers to gain access to the system. Key logging is the practice of noting the keys struck on keyboard, typically in manner so that person using the system keyboard is unaware that such action is monitored. There are two types of key loggers viz. software key logger and hardware key logger. Software key loggers are installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded. Textual passwords have been the most widely used authentication method for decades. Textual passwords Comprised of numbers and upper-case and lower-case Alphabets, textual passwords are considered strong enough to resist against brute force attacks. However, a strong textual password is hard to memorize and recollect [1]. Therefore, users tend to choose passwords that are either short or from the dictionary, 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 [2]. 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 [3]. 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 the 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. The human actions such as choosing wrong passwords for new accounts and entering passwords in an insecure way for later logins are regarded as the weakest link in the authentication chain [4]. Therefore, an authentication scheme should be designed to overcome these vulnerabilities. In this project, we proposed 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. The shoulder surfing attack is an attack that can be performed by the adversary to obtain the user's password by watching over the user's shoulder as he enters his password. As conventional password schemes are vulnerable to shoulder surfing attacks, we are proposing shoulder surfing resistant graphical password schemes using Pass Matrix.

2. LITERATURE SURVEY

Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng:"A Shoulder Surfing Resistant Graphical Authentication System": Authentication based on passwords is used largely in applications for computer security and privacy. However, human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as "the weakest link" in the authentication chain. Rather than arbitrary alphanumeric strings, users tend to choose passwords either short or meaningful for easy memorization. With web applications and mobile apps piling up, people can access these applications anytime and anywhere with various devices. This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' credentials. To overcome this problem, we proposed a novel authentication system PassMatrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, PassMatrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks. We also implemented a PassMatrix prototype on Android and carried out real user experiments to evaluate its memorability and usability. From the experimental result, the proposed system achieves better resistance to shoulder surfing attacks while maintaining usability.

Mughele, Ese and Sophia:"Three level password authentication" Authentication is one of the most important security service provided to system by the different authentication schemes or algorithms which must be provided so that only authorized persons can have right to use or handle that system and data related to that information system securely. Techniques used include Token based, biometric based as well as knowledge based. Despite these, no single mechanism is efficient and effective to provide adequate security for computing resources such as programs, files, messages, printers, internet, etc. A three- level authentication is proposed in this paper that is more confidential for ensuring adequate security.

Novel Shoulder-Surfing Resistant Authentication Schemes using Text-Graphical Passwords: There are many applications which require the user to be authenticated before being permitted to perform certain tasks. Text password based authentication is a popularly used authentication mechanism. Despite having greater security, text passwords are characterized by selection of a weak and easy to remember passwords. Users tend to write them down and share them with friends, family members and colleagues defeating the security provided by text-passwords. Graphical passwords offer an alternative to text passwords as the password space is typically higher, less prone to dictionary attacks and easier to remember visually. However, they suffer from shoulder-surfing attacks. In this paper, we propose two authentication schemes that support keyboard as well as graphical mouse-based input that map password characters to other regions of the password space. This shields the user's password from being known to the adversary thus deflecting shoulder surfing and spyware attacks. The schemes include both single and multi colour input images consisting of printable characters. An analysis of security, usability, memorability and social engineering aspects of the proposed schemes is presented. Future research directions are also presented.

A. Paivio, T. Rogers, and P. Smythe, "Why are pictures easier to recall than words?" Pictures of objects were recalled significantly better than their names on the first two of four free recall trials. Recall for the two modes did not differ in intertribal organization but striking differences occurred as a function of input serial order. Picture superiority occurred for terminal input items on Trial 1, and both terminal and early items on Trial 2. The findings are discussed in terms of verbal and nonverbal (concrete) memory codes.

S.Brostoff and M. Sasse, "Are passfaces more usable than passwords? A field trial investigation," The proliferation of technology requiring user authentication has increased the number of passwords which users have to remember, creating a significant usability

problem. This paper reports a usability comparison between a new mechanism for user authentication — Passfaces — and passwords, with 34 student participants in a 3-month field trial. Fewer login errors were made with Passfaces, even when periods between logins were long. On the computer facilities regularly chosen by participants to log in, Passfaces took a long time to execute. Participants consequently started their work later when using Passfaces than when using passwords, and logged into the system less often. The results emphasize the importance of evaluating the usability of security mechanisms in field trials.

S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," Computer security depends largely on passwords to authenticate human users. However, users have difficulty remembering passwords over time if they choose a secure password, i.e. a password that is long and random. Therefore, they tend to choose short and insecure passwords. Graphical passwords, which consist of clicking on images rather than typing alphanumeric strings, may help to overcome the problem of creating secure and memorable passwords. In this paper we describe PassPoints, a new and more secure graphical password system. We report an empirical study comparing the use of PassPoints to alphanumeric passwords. Participants created and practiced either an alphanumeric or graphical password. The participants subsequently carried out three longitudinal trials to input their password over the course of 6 weeks. The results show that the graphical password users created a valid password with fewer difficulties than the alphanumeric users. However, the graphical users took longer and made more invalid password inputs than the alphanumeric users while practicing their passwords.

D. Nelson, U. Reed, and J. Walling," picture superiority effect in associative recognition: Previous research has shown that the picture superiority effect (PSE) is seen in tests of associative recognition for random pairs of line drawings compared to pairs of concrete words (Hockley, 2008). In the present study we demonstrated that the PSE for associative recognition is still observed when subjects have correctly identified the individual items of each pairas old (Experiment 1), and that this effect is not due to rehearsal borrowing (Experiment 2). The PSE for associative recognition also is shown to be present but attenuated for mixed picture-word pairs (Experiment 3), and similar in magnitude for pairs of simple black and white line drawings and coloured photographs of detailed objects (Experiment 4). The results are consistent with the view that the semantic meaning of nameable pictures is activated faster than that of words thereby affording subjects more time to generate and elaborate meaningful associations between items depicted in picture form. (PsycINFO Database Record (c) 2016 APA, all rights reserved).

3. EXISTING TECHNIQUES

In the existing system there were several methods that were used for providing security for the data. Initially we try to use the password based authentication which is no longer providing high level of security, Later we applied graphical password based authentication by taking images as input for providing security, but they were also failed in some areas. 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 [3]. Textual passwords are often insecure due to the difficulty of maintaining strong ones. Textual passwords have been the most widely used authentication method for decades Comprised of numbers and upper and lower-case letters, textual passwords are considered strong enough to resist against brute force attacks. However, a strong textual password is hard to memorize and recollect. Therefore, users tend to choose passwords that are either short or from the dictionary, rather than random alphanumeric strings.

4. OVERVIEW OF PROPOSED METHOD

This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' credentials. To overcome this problem, we proposed

a novel authentication system Pass Matrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, Pass Matrix offers no hint for attackers to figure out or narrow-

down the password even they conduct multiple camera-based attacks. Various graphical password authentication schemes were developed to address the problems and weaknesses associated with textual passwords. Based on some studies, it specifies that 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 the memory is not activated periodically. 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.

5. EXPERIMENTAL STUDY

5.1 Multi Layer Image Authentication

To overcome the security weakness of the traditional PIN method, the easiness of obtaining passwords by observers in public, and the compatibility issues to devices, we introduced a graphical authentication system called PassMatrix. In PassMatrix, a password consists of only one pass-square per pass-image for a sequence of n images. The number of images (i.e., n) is user-defined. Bellow figure demonstrates the proposed scheme, in which the first pass-square is located at in the first image, the second pass-square is on the top of the smoke in the second mage at , and the last pass-square is at in the third image. In PassMatrix, users choose one square per image for a sequence of n images rather than n squares in one image as that in the Pass Points scheme. Based on the user study on Cued Click Points. CCP method does a good job in helping users recollect and remember their passwords. If the user clicks on an incorrect region within the image, the login will be failed.

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

5.2 PASSMATRIX AUTHENTICATION

In PassMatrix, a password consists of only one pass-square per pass-image for a sequence of n images. The number of images (i.e., n) is user-defined. Figure 5 demonstrates the proposed scheme, in which the first pass-square is located 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. In PassMatrix, users choose one square per image for a sequence of n images rather than n squares in one image as that in the PassPoints scheme.

PassMatrix is composed of the following components (seeFigure 5.2):

Image Discretization Module

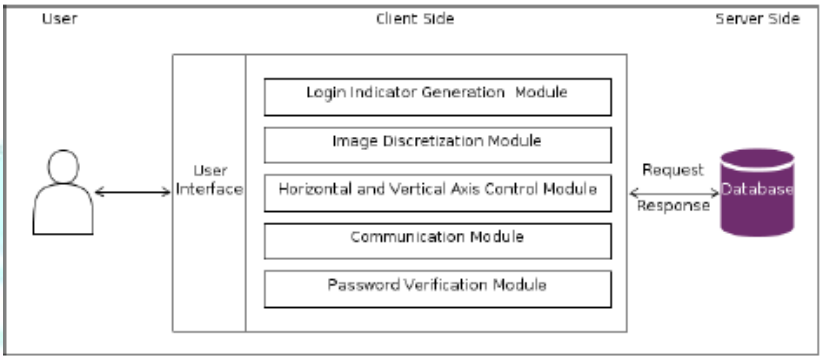
Horizontal and Vertical Axis Control Module

Login Indicator generator Module

Communication Module

Password Verification Module

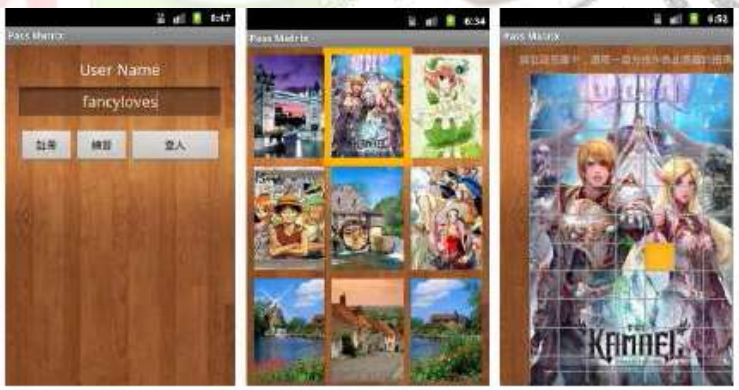
Database



PASSMATRIX (Figure 5.2)

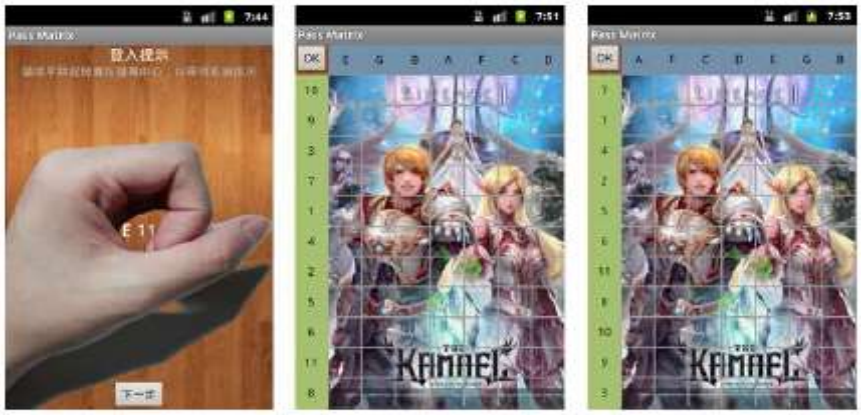
Grid Image Authentication

In this type of authentication multiple images can be provided to the user, the user has the select the image that he can to log in, this will the provide more security.



(a) Obtain the login indicator (E,11) directly.

(b) Obtain the loginindicator through a predefined image



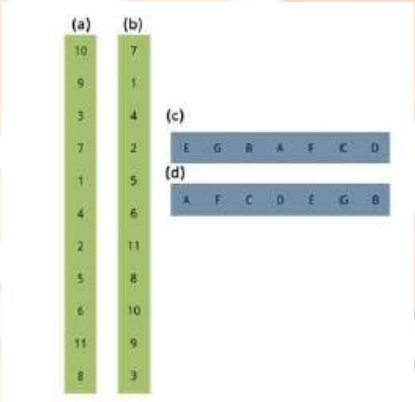
(a) The Main page of PassMatrix, users can register an account,practice or start to log in for experiment.

(b) Users can choose from alist of 24 images as their pass-images.

(c) There are 7 X 11 squares ineach image, from which users choose one as the pass-square.

Color Image Authentication

In this type the authentication is used by the color coordinates of that position. In normal Authentication the password is setting according to the regions. But in this type of authentication we choose the color coordinates for password setting



Horizontal scroll bar (on the right/blue) and vertical bar (on theleft/green)

Random Guess Attack

To perform a random guess attack, the attacker randomly tries each square as a possible pass-square for each pass image until a successful login occurs. The key security determinants of the system are the number of pass-images and the degree of discretization of each image. To quantify the security of PassMatrix against random guess attacks, we define the entropy of a password space as in equation3. Table 7 defines the notations used in the equation. If the entropy of a password space is k bits, there will be 2kpossible passwords in that space.

Entropy = log2((Dx_ Dy)i)n

TABLE 7
The definition of notations used in equation 3.

Notation	Definition
D_x	The number of partitions in x-direction
D_y	The number of partitions in y-direction
i=1	Obtain login indicators by touching the screen with hand grasped
i=2	Obtain login indicators by predefined images
n	The number of pass-images set by user

6. CONCLUSION

In this Thesis we have studied different methods for graphical password authentication scheme. We proposed a Shoulder surfing resistant authentication system based on graphical passwords, named PassMatrix. Using a one-time login indicator per image, users can point out the location of their pass-square without directly clicking or touching it,which is an action vulnerable to shoulder surfing attacks. Because of the design of the horizontal and vertical bars thatcover the entire pass-image, it offers no clue for attackers to narrow down the password space even if they have morethan one login records of that account. Furthermore, we will implement a PassMatrix prototype on windows andcarried out user experiments to evaluate the memorability and usability. With the increasing trend of web services and apps, users are able to access these applications anytime and anywhere with various devices. In order to protect users' digital property, authentication is required every time they try to access their personal account and data. However, conducting the authentication process in public might result in potential shoulder surfing attacks. Even a complicated password can be cracked easily through shoulder surfing. Using traditional textual passwords or PIN method, users need to type their passwords to authenticate themselves and thus these passwords can be revealed easily if someone peeks over shoulder or uses video recording devices such as cell phones.

REFERENCES

[1] S. Sood, A. Sarje, and K. Singh, "Cryptanalysis of passwordauthentication schemes: Current status and key issues," in Methodsand Models in Computer Science, 2009. ICM2CS 2009.Proceeding ofInternational 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), 2014International 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/mobilemarketing/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 InteractionSpecial 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.

AUTHORS

Shiva Pampana
Department of CST,
A.U.College of Engineering (A)
Andhra University,
Visakhapatnam

Prof. Kasukurthi Venkata Rao
Department of CS & SE,
A.U.College of Engineering (A)
Andhra University, Visakhapatnam