ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

A Survey on Shoulder Surfing Resistant Graphical Authentication Systems

Tejashri Dumbre[1], Prof. S. A. Kahate[2]

M.E. Student, Dept. of Computer Engineering, SPCOE, Otur, Pune, Maharashtra, India[1]

Assistant Professor, Dept. of Computer Engineering, SPCOE, Otur, Pune, Maharashtra, India[2]

ABSTRACT: Authentication based on passwords is used largely in applications for computer security and privacy. However, humanactions such a choosing wrong passwords and inputted passwords in an not secure way are regarded as" the weakest connection" in theauthentication chain. Rather than arbitrary alphanumeric character, users tend to select a password either short or his name related for easymemorization. With web site applications and mobile phone apps charging up, peoples can get access this typeof application anytime and anywhere with multiple devices. This evolution brings good convenience but also improves the probability of exposing passwords to shoulder surfingattacks. Attackers can observe directly or use external recording devices to collect users' credentials. To come this problem, weproposed a novel authentication system Pass Matrix, based on graphical passwords to resist shoulder surfing attacks. Many authentications methods are presented, but users are familiar with textual password method. Textual password methods are vulnerable to shoulder surfing andkey loggers. To come this problem many other authentication system like token based authentication, biometric bases authentication systems, graphical password methods have been proposed. In pair based system, the proposed of session password scheme uses Text and colors for generating session password. In the proposed scheme, theuser can easily and efficiently login system.

KEYWORDS: Graphical Passwords, Authentication, Shoulder Surfing Attack, Pair-based Authentication scheme.

I. Introduction

Shoulder surfing technique of gathering information such as usernames and passwords by watching over a person's shoulder while he/she logs into the system, thereby helping attackers to gain anaccess 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 keyloggers viz. software key logger and hardware keylogger. Software keylogger is 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. 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. 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. 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 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 not secure way for later logins are regarded as the weakest link in the authentication chain. Therefore, an authentication scheme should be designed to overcome these vulnerabilities. In this project, we purposed a secure graphical authentication system named Pass-Matrix that protects

DOI: 10.15680/IJIRCCE.2016. 0411236

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 pointout the position of their passwords rather than clicking on the password object directly.

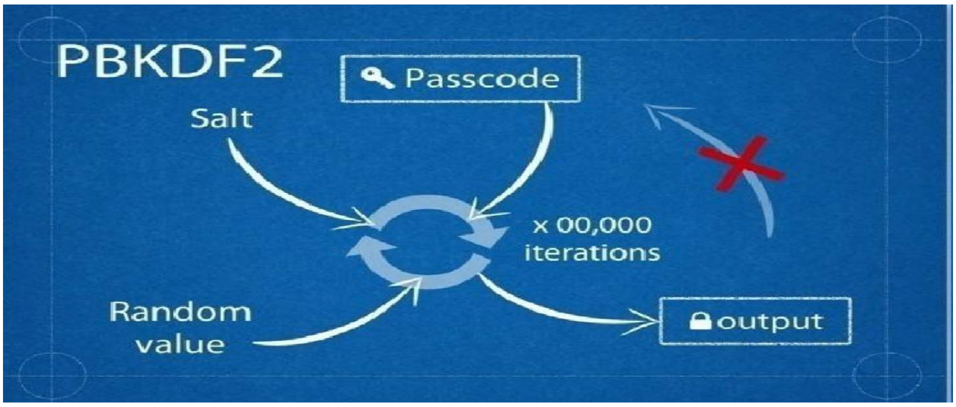

Figure 1: Password based encryption in pair based system.

The shoulder surfing attack in 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, Sobrado and Birget proposed three shoulder surfing resistant graphical password schemes. Since then, many graphical password schemes with different degrees of resistance to shoulder surfing have been proposed, and each has its pros and cons. seeing that most users are more familiar with textual passwords than pure graphical passwords.

II. Literature Survey

1. An Association –BasedGraphical Password Design Resistant to Shoulder-Surfing Attack

Author presents a novel graphical password design in this paper [2]. It rests on the human cognitive ability of association-based memorization to make the authentication more user-friendly, comparing with traditional textual password. Based on the principle of zero-knowledge proof protocol, we further improve our primary design to overcome the shoulder-surfing attack issue without adding any extra complexity into the authentication procedure. System performance analysis and comparisons are presented to support our proposals.

2. Pass - thoughts: authenticating with our minds.

Author presents a novel idea for user authentication that we callpass-thoughts [3]. Recent advances in BrainComputer Interface (BCI) technology indicate that there is potentialfor a new type of human-computerinteraction: a user transmitting thoughts directly to a computer.The goal of a pass-thought system wouldbe to extract as much entropy as possible from a user’s brain signals upon“transmitting” a thought.Provided that these brain signals can be recorded and processed in an accurate and repeatable way,a pass-thought system might provide a quasi two-factor, changeable, authentication method resilient toshoulder-surfing. The potential size of the space of a pass-thought system would seem to be unbounded intheory, due to the lack of bounds on what composes a thought, although in practice it will be finite due tosystem constraints. In this paper, author discuss the motivation and potential of pass-thought authentication,the status quo of BCI technology

3. A User Study Using Images for Authentication.

Current secure systems suffer because they neglect the importance of human factors in security. Author addressesa fundamental weakness of knowledge-based authentication schemes, which is the human limitation to remember secure passwords. Our approach to improve the security of these systems relies onrecognition-based,rather thanrecall-based authentication [10]. Author examines therequirements of a recognition-based authentication system and proposes is more reliable and easier to use than traditional recall-based schemes, which require the user toprecisely recall passwords or PINs. Furthermore, it hasthe advantage that it prevents users from choosing weakpasswords and makes it difficult to write down or sharepasswords with others.

4. The design and analysis of graphical passwords

In this paper author propose and evaluate new graphical password schemes that exploit features of graphical input displays to achieve better security than text-based passwords [11]. Graphical input devices enable the user to decouple the position of inputs from the temporal order in which those inputs occur, and we show that this decoupling can be used to generate password schemes with substantially larger (memorable) password spaces. In order to evaluate the security of one of our schemes, we devise a novel way to capture a subset of the "memorable" passwords that, we believe, is itself a contribution.

5. Shoulder surfing by using gaze -based password entry, Proceedings

In 2002, Sobrado and Birget [6] proposed three shouldersurfing resistant graphical password schemes, the Movable Frame scheme, the Intersection scheme, and the Trianglescheme. However, both the Movable Frame scheme and theIntersection scheme have high failure rate. In the Trianglescheme, the user has to choose and memorize several passiconsas his password. To login the system, the user has tocorrectly pass the predetermined number of challenges. Ineach challenge, the user has to find three pass-icons among a set of randomly chosen icons displayed on the loginscreen, and then click inside the invisible triangle createdby those three pass-icons.

Sr. No	Paper Name	Author Name	Descriptions	Year
1	Association –Based Graphical Password Design Resistant to Shoulder-Surfing Attack	Zhi Li, Qibin Sun, Yong Lian, and D. D. Giusto	In this paper, it rests on the human cognitive ability of association-based memorization to make the authentication more user-friendly, comparing with traditional textual password.	2005
2	Pass - thoughts: authenticating with our minds.	Julie Thorpe P.C. van Oorschot Anil Somayaji	Author present a pass-thought system would be to extract as much entropy as possible from a user's brain signals upon "transmitting" a thought. Provided that these brain signals can be recorded and processed in an accurate and repeatable way, a pass-thought system might provide a quasi two-factor, changeable, authentication method resilient to shoulder-surfing.	2005
3	A User Study Using Images for Authentication.	RachnaDhamija Adrian Perrig	Author addresses a fundamental weakness of knowledge-based authentication schemes, which is the human limitation to remember secure passwords. Our approach to improve the security of these systems relies on recognition-based, rather than recall-based authentication	2013
4	The design and analysis of graphical passwords		In this paper author propose and evaluate new graphical password schemes that exploit features of graphical input displays to achieve better security than text-based passwords	2012
5	Shoulder surfing by using gaze -based password entry, Proceedings	Sobrado and Birget	Author proposed three shoulder surfing resistant graphical password schemes, the Movable Frame scheme, the Intersection scheme, and the Triangle scheme. However, both the Movable Frame scheme and the Intersection scheme have high failure rate.	2002

Table 2.1: Literature survey

DOI: 10.15680/IJIRCCE.2016. 0411236

III. **PORPOSED SYSTEM**

In Pass Matrix, users choose one square per image for a sequence of n images rather thann squares in one image as that in the Pass-Points scheme. Based on the user study ofCued Click Points. However, aiming at alleviating shoulder surfing attacks, we do notrecommend this approach since the feedback that is given to users might also be obtainedby attackers. Due to the fact that people do not register a new account or set up a newscreen lock frequently, we assume that these setup events can be done in a safe environmentrather than in public places. Thus, users can pick up pass-squares by simple touching at or clicking on them during the registration phase.

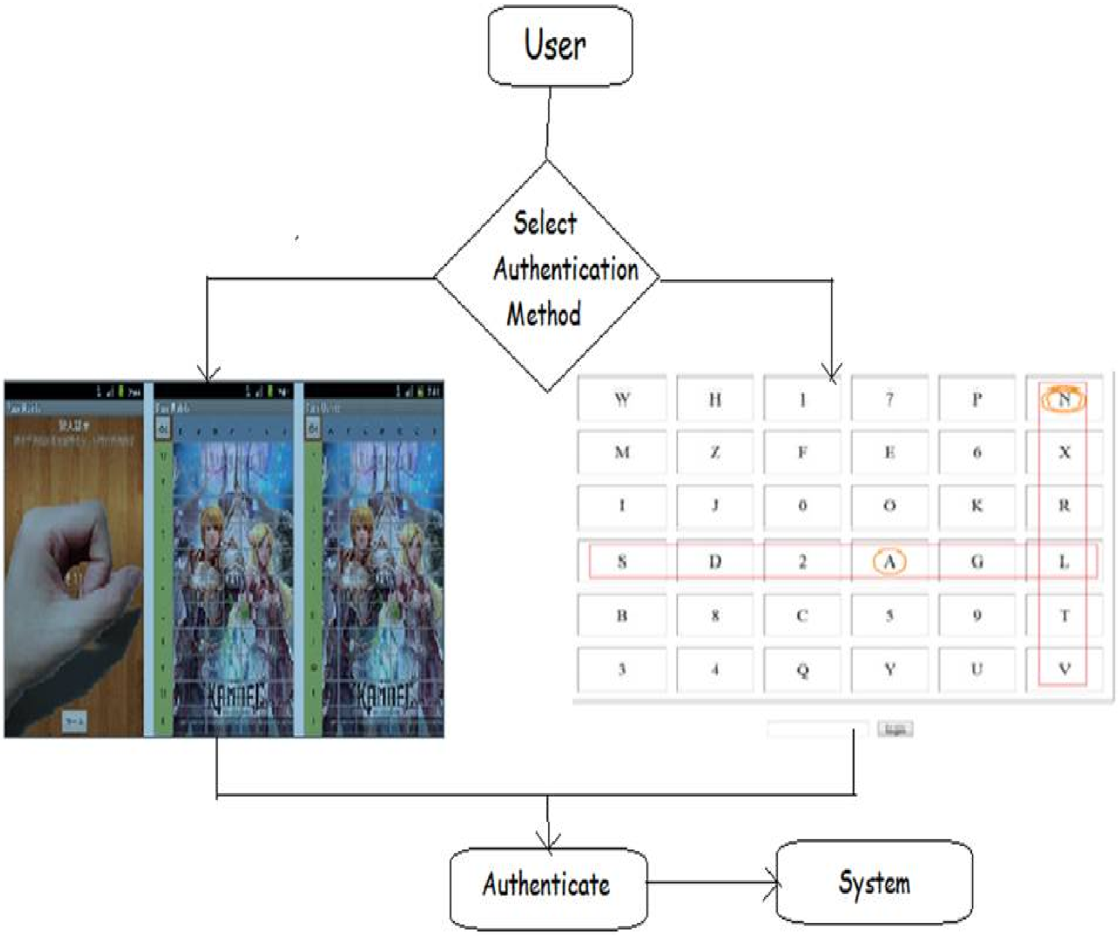

Figure 1:System Flow

To overcome (1) the security weakness of the traditional PIN method, (2) the easiness of obtaining passwords by observers in public, and (3) the compatibility issues to devices, we introduced a graphical authentication system called Pass-Matrix. In Pass-Matrix, 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 2 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

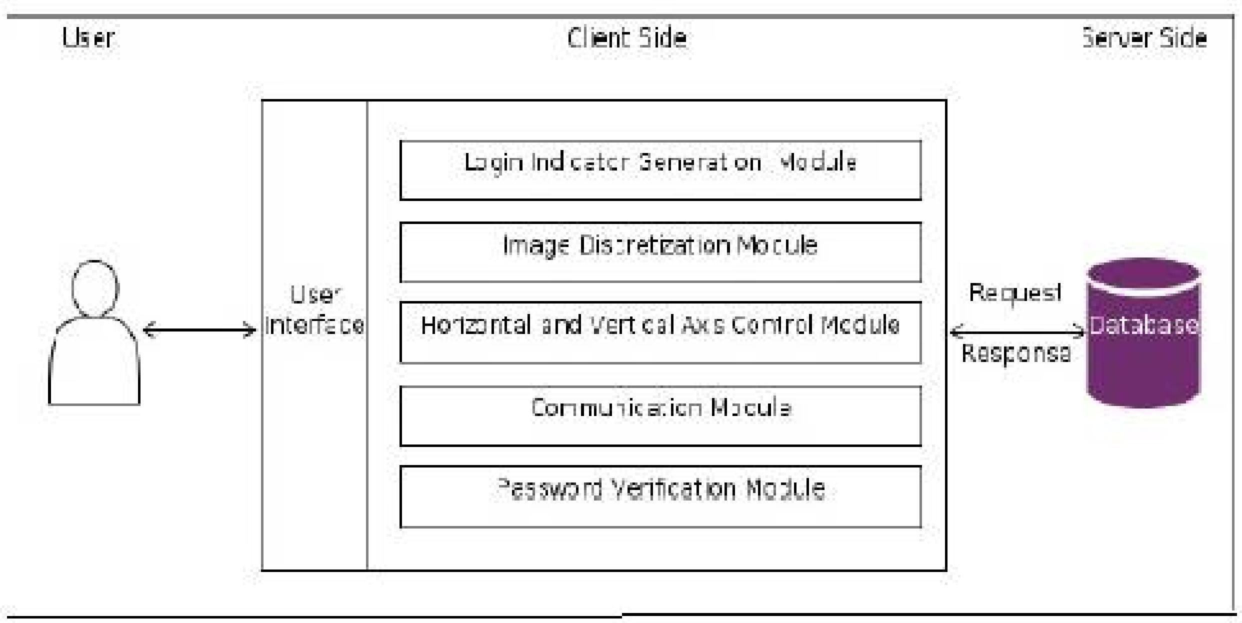
User
Client Side
Server Side
User Interface
Login Indicator Generation Module
Image Discretization Module
Horizontal and Vertical Axis Control Module
Communication Module
Password Verification Module
Request
Response
Database

Fig.2 System Architecture

IV. CONCLUSION

In this paper, we have studied different methods for graphical password authentication scheme. We proposed a shoulder surfing resistant authentication system basedon graphical passwords, named Pass Matrix. 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 thehorizontal and vertical bars that cover the entire pass-image, it offers no clue for attackersto narrow down the password space even if they have more than one login records ofthat account. Also additional, we proposed a system called Session password,it provides a new password for each session and need not to transfer password form server each time for authentication purpose that's why Session password scheme provides more security than the other existed systems.

REFERENCES

1. XiaoyuanSuo, Ying Zhu G. Scott. Owen 2005, 'Graphical passwords: a survey', 21st Annual Computer Security Applications Conference.
2. ZhiLi ,Qibin Sun , Yong Lian , and D. D. Giusto , 2005, 'An Association –BasedGraphical Password Design Resistant to Shoulder-Surfing Attack', IEEE InternationalConference on Multimedia and Expo (ICME).
3. Julie Thrope, P. C. van Oorschot, Anil Somayaji, 2005, 'Pass - thoughts: authenticating with our minds', Proceedings of the 2005 workshop on New security paradigms,ACM.
4. Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, Jean -Camille Birget, 2006,'Design and Evaluation of a Shoulder -Surfing Resistant Graphical PasswordScheme',Proceedings of Advanced Visual Interfaces (AVI2006).
5. Furkan, Tari, A. Ant Ozok, Stephen H. Holden, 2006, 'A comparison of perceived and real shoulder -surfing risks between alphanumeric and graphical passwords', Proceedingsof the second symposium on Usable privacy and security, ACM.
6. Di Lin, Paul Dunphy, Patrick Olivier, JeYan, 2007, 'Graphical password s & qualitativespatial relations',Proceedings of the 3rd symposium on Usable privacy andsecurity, ACM.
7. Manu Kumar, Tal Garnkel, Dan Boneh, Terry Winograd, 2007, 'Reducing shoulder surfing by using gaze -based password entry', Proceedings of the 3rd s symposium onUsable privacy and security, ACM.
8. Cheryl, Hinds and ChineduEkwueme, 2007, 'Increasing security and usability ofcomputer systems with graphical passwords', Proceedings of the 45th annual southeast regional conference, ACM.
9. Huanyu Zhao a ndXiaolin Li , 2007, 'S3PAS: A Scalable Shoulder - Surfing ResistantTextual -Graphical Password Authentication Scheme', 21st International Conferenceon Advanced Information Networking and Applications Workshops (AINAW).
10. SarangaKomanduri and Dugald R. Hutchings, 2008, 'Order and entropy in picturepasswords', Proceedings of graphics interface, Canadian Information ProcessingSociety.
11. Paul Dunphy, James Nicholson, Patrick Oliver,2008, 'Securing passfaces for description',Proceedings of the 4th symposium on Usable and security, ACM.
12. R. Dhamija, and APerrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.
13. Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin., "The design and analysis of graphical passwords" in Proceedings of USENIX Security Symposium, August 1999.

.

DOI: 10.15680/IJIRCCE.2016. 0411236