A Review on – Shoulder Surfing Resistant Graphical & Pair Based Authentication System

Shaikh Mudassir[1], Rohan Khaire[2]

Asst Professor[1], P.G. Student[2],Department of Computer Science & Engineering, Everest College of Engineering & Technology, Aurangabad, Maharashtra, India

Abstract— **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. With the increasing amount of mobile devices and web services, users can access their personal accounts to send confidential business emails, upload photos to albums in the cloud or remit money from their e-bank account any time and anywhere. While logging into these services in public, they may expose their passwords to unknown parties unconsciously. People with malicious intent could watch the whole authentication procedure through omnipresent video cameras and surveillance equipment, or even a reflected image on a window. Once the attacker obtains password, they could access personal accounts and that would definitely pose a great threat to ones assets. Shoulder surfing attacks have gained more and more attention in the past decade.**

Keywords: *Pass matrix, paired based, Image Discretization, authentication.*

I INTRODUCTION

Now a day's hundreds of millions of peoples using internet daily and day by day they are increasing. Today for authentication user name and password is used the basically. so the security must be provided in order to prevent hackers from accessing the account data. So authentication must be secure in order to protect user accounts. Authentication is provided by using two new techniques i.e. pair based authentication scheme, hybrid textual authentication scheme. The user has to select the authentication scheme at a time of login.

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, pass matrix and paired passed proposed shoulder surfing resistant graphical pass- word 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 password. Our solution will provide an improved text-based shoulder surfing resistant graphical password scheme by using colors. The operation of the proposed scheme is simple and easy to learn for users familiar with textual passwords. The user can easily and efficiently to login the system without using any physical keyboard or on-screen keyboard.

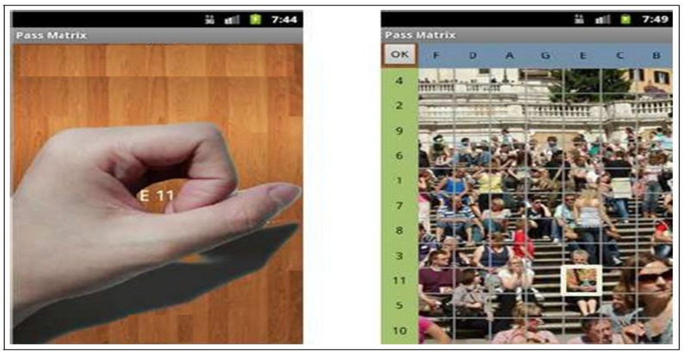

Figure 1: Login indicator

Human factors are often considered the weakest link in a computer security system. Patrick, et al. point out that there are three major areas where human computer interaction is important: authentication, security operations, and developing secure systems. Here we focus on the authentication problem.

Current authentication methods can be divided into three main areas:

- Token based authentication
- Biometric based authentication
- Knowledge based authentication
  -Text based authentication
  -Picture based authentication

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number. Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security. Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. The most common knowledge based authentication method is for a user to submit a user name and a text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember [2]. Unfortunately, these passwords can also be easily guessed or broken. According to a recent Computerworld news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords [3]. On the other hand, passwords that are hard to guess or break are often hard to remember. Thus a large portion of customer service calls are related to one’s forgetting his or her password. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts [4, 5]. Recently security researchers have detected a rise in the spread of Key logger [6], a spyware built to capture login names and passwords and to send them to the attackers. Text-based passwords are particularly vulnerable to such attacks. To address the problems with traditional username-password authentication, alternative authentication methods, such as biometrics [3, 7], have been used. In this paper, however, we will focus on another non-traditional authentication method: using pictures as passwords.

II LITERATURE SURVEY

In recognition based techniques, users are given a set of pictures and they pick and memorize some of them. During authentication, the users need to recognize and identify the pictures they have picked earlier. Dhamija and Perrig [4] proposed an graphical authentication scheme based on Hash Visualization technique [9]. In their system, user will be asked to select certain number of images from a set of random pictures generated by a program (figure 1). Later, user will be required to identify the pre-selected images to be authenticated. The results showed that 90% of all participants succeeded in the authentication using their technique, while only 70% succeeded using text-based passwords and PINS. The average log-in time, however, is longer than the traditional approach, but has a much smaller failure rate. A drawback is that the server needs to store a large amount of pictures which may have to be transferred over the network, delaying the authentication process. Another weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Interface-wise, the process of selecting a picture from picture database can be tedious and time consuming for the user.

In Akula and Devisetty’s algorithm [10], the system displays a set of images to the user and the user would then select the correct pass-image. The basic scheme is similar to the technique proposed by Dhamija and Perrig [4]. The difference is that this technique uses the hash function SHA-1, which produces a 20 byte output. This makes the authentication secure and requires less memory. However, an image file still occupies more space than text even after hashing. The authors suggested a possible future improvement by providing the persistent storage and this could be deployed on the Internet, cell phones and PDA's. Weinshall and Kirkpatrick [11] identified a wide range of human memory phenomena as potential certificates of identity. They sketched several authentication schemes, such as picture recognition, object recognition, and pseudo word recognition, and conducted a number of user studies. In the picture recognition study, a user is trained to recognize a large set of images (100 – 200 images) selected from a database of 20,000 images. After one to three months, users in their study were able to recognize over 90% of the images in the training set.

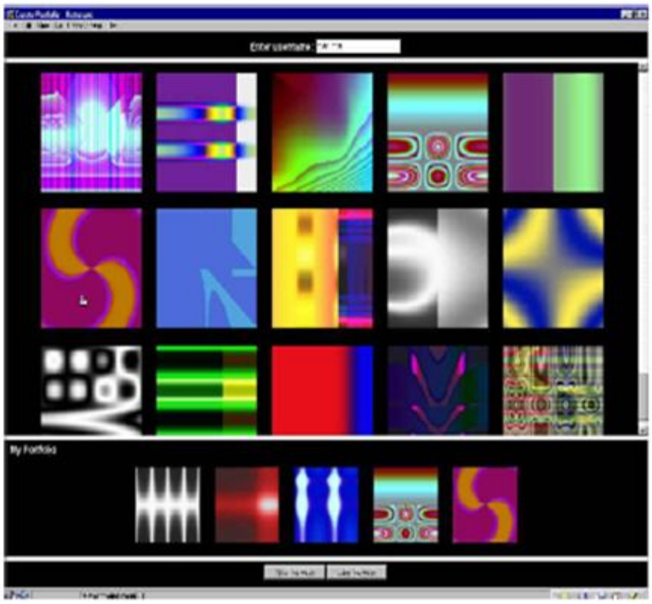

Figure 2 Random arts used by Dhamija and Perrig [4]

This study showed that pictures are the most effective among the three schemes tested. Pseudo codes can also be used, but require proper setting and training. Sobrado and Birget [12] developed a graphical password technique that deals with shoulder-surfing problem. In the first scheme, the system will display a number of pass objects (pre-selected by user) among many other objects. To be authenticated, a user needs to recognize pass-objects and click inside the convex hull formed by all the pass objects (figure 2). In order to make the password hard to guess, Sobrado and Birget suggested using 1000 objects, which making the display very crowded and the objects almost indistinguishable. On the other hand, using fewer objects may lead to a smaller password space, since the resulting convex hull can be large. In their second algorithm, a user moves a frame (and the objects within it) until the pass object on the frame lines up with the other two pass-objects. The authors also suggest repeating the process for a few more times to minimize the likelihood of logging in by randomly clicking or rotating. The main drawback of these algorithms is that the log in process can be slow.

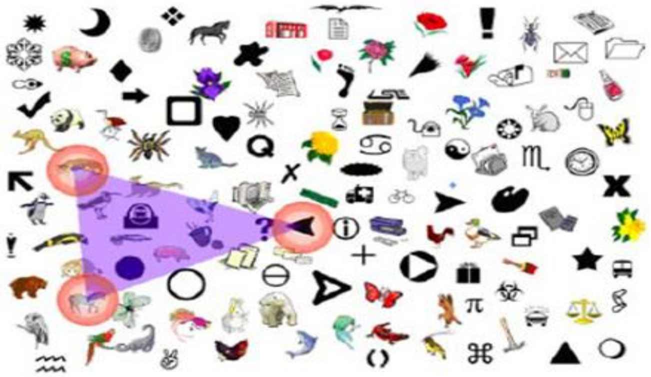

Figure 3 A shoulder-surfing resistant graphical password scheme. (Source: Sobrado and Birget [12])

Man, et al. [14] proposed another shoulder-surfing resistant algorithm. In this algorithm, a user selects a number of pictures as pass-objects. Each pass-object has several variants and each variant is assigned a unique code. During authentication, the user is challenged with several scenes. Each scene contains several pass-objects (each in the form of a randomly chosen variant) and many decoy-objects. The user has to type in a string with the unique codes corresponding to the pass-object variants present in the scene as well as a code indicating the relative location of the pass-objects in reference to a pair of eyes. The argument is that it is very hard to crack this kind of password even if the whole authentication process is recorded on video because where is no mouse click to give away the pass-object information. However, this method still requires users to memorize the alphanumeric code for each pass-object variant. For example, if there are 4 pictures each with 4 variants, then each user has to memorize 16 codes. Although the pass-objects provide some cues for recalling the codes, it is still quite inconvenient.

III CONCLUSION

With the increasing trend of web services and apps, users are able to access these applications anytime and anywhere with various devices. However, conducting the authentication process in public might result in potential shoulder surfing attacks. Our system is a combination of recognition and recall based approach. It is more usable and secure as compare to previous graphical password authentication systems . As password space is very large it provides the security against brute force attack. It is easy to use. Passwords can be created and memorized easily .

Randomization in both the authentication steps provides strong security against shoulder surfing. Overall our system is resistant to all other possible attacks also. This system can be used for highly secure systems. In future, one more addition possible to our system is, if the user forgets any password that password is mailed to user's registered mail id and such a message will be sent to user's registered mobile number also. So user can get the system updates although he is offline. Thus, in future, our system can be made more secure and easy to access.

REFERANCES

[1] A. C. L. Andrew S. Patrick, Scott Flinn, "HCI and Security Systems," in CHI,
Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA., 2003.

[2] A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise
computer security mechanisms and how to take remedial measures," *Communications of*
the ACM, vol. 42, pp. 41-46, 1999.

[3] K. Gilhooly, "Biometrics: Getting Back to Business," in *Computerworld, May 09*,
2005.

[4] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for
Authentication," in *Proceedings of 9th USENIX Security Symposium*, 2000.

[5] M. Kotadia, "Microsoft: Write down your passwords," in *ZDNet Australia, May*
23, 2005.

[6] A. Gilbert, "Phishing attacks take a new twist," in *CNET News.com, May 04*,
2005.

[7] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," *Communications of*
the ACM, vol. 33, pp. 168-176, 2000.

[8] R. N. Shepard, "Recognition memory for words, sentences, and pictures," *Journal*
of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163, 1967.

[9] A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-
World Security," in *Proceedings of the 1999 International Workshop on Cryptographic*
Techniques and E-Commerce, 1999.

[10] S. Akula and V. Devisetty, "Image Based Registration and Authentication
System," in *Proceedings of Midwest Instruction and Computing Symposium*, 2004.
57