Volume 4, Issue 4, April 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Study of Implementation of Image Based Authentication System

[1]Manish Kumar,
[1]M.Tech Scholar,
Subharti Institute of Technology and Engineering,
Meerut, India

[2]Prof (Dr.) Jayant Shekhar
[2]Principal,
Subharti Institute of Technology and Engineering,
Meerut, India

Abstract: ***The paper aims on the study of a system for user authentication based on the use of images as passwords. The proposed method is thought to solve the traditional problems related to the authentication process in the Internet environment by exploiting the human brain's remarkable ability in image recognition. Authentication plays a very important role in protecting resources against unauthorized use. Many authentication processes exist from simple password based authentication system to costly biometric authentication systems. So when increasing security is an issue text based passwords are not enough to tackle such problems. The need for something more secure along with being user friendly is required. The image password demonstrates to be more secure than the common alphanumeric password and at the same time more easy-to-use. In this paper, we conduct a comprehensive survey of the existing graphical password techniques and comparing both alphanumeric and graphical passwords. We classify these techniques into two categories: recognition-based and recall-based approaches. We discuss the strengths and limitations of each method and point out the future research directions in this area. We also try to answer two important questions: "Are graphical passwords as secure as text-based passwords?"; "What are the major design and implementation issues for graphical passwords?"This survey will be useful for information security researchers and practitioners who are interested in finding an alternative to text-based authentication methods.***

Keywords: biometric, images, passwords, authentication, security etc

1. INTRODUCTION

Human factors are often considered the weakest link in a computer security system. Patrick, et al. [1] point out, that there are three major areas where human-computer interaction is important: authentication, security operations, and developing secure systems. Here, we basically focus on the authentication problem. The most common computer authentication method for a user is to submit a user name and a text password. The vulnerabilities of this method have been well known to all of us. So, one of the main problems is the difficulty of remembering passwords [2]. Several Surveys have shown that users tend to pick short passwords or passwords that are easy to remember [3]. Unfortunately, these passwords can also be easily guessed or broken. According to a Computerworld recent news article, the essential problem is this: The more complex a password is, the harder it is to guess, and the more secure it is. But the more complex a password is, the more likely it is to be written down, shared or otherwise stored in an easily accessible location, and therefore the *less* secure it is. And the killer corollary: If a password is stolen, its relative simplicity or complexity becomes irrelevant. In a carefully worded blog post, LinkedIn director Vicente Silveira said the company has confirmed that an unspecified number of hashed passwords posted publicly on a Russian hacker forum earlier this week, "correspond to LinkedIn accounts"[4].On the other hand, passwords that are hard to guess or break are often hard to remember. 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 [5, 6]. For addressing the problems with traditional username and password authentication alternative methods like biometrics [7], have been used. However, in this paper we will focus on another alternative using image as passwords and we want to answer the following questions:

- Are graphical passwords as secure as text passwords?
- What are the major design and implementation issues for graphical passwords?

2. RELATED WORK : HISTORY

There are two fields of work related to photographic authentication. Firstly, graphical passwords and Secondly, authentication over untrusted channels. The basic idea of using graphical systems for authentication is not new. But no prior research has explored using the personal photograph collections. Similarly, some previous work has been done which investigates information on untrusted terminals, but this work has no concern with the authentication process.

There are some graphical or image based authentication approaches proposed in different literature. In [6], a user is required to point out some predetermined coordinates on an image ("graphical password") in some particular order for being authenticated. Also, two graphical password schemes were proposed in [9]. The first method was enhancement of the input of text based passwords using graphical techniques. The second method requires from user to draw a secret design on some display grid. These schemes achieved better security as compared to conventional textual passwords. The requirements of recognition based authentication system were examined in [5]. In this approach, the authentication depends on user's ability to recognize the images which are seen previously. An interface which is similar to a numeric

keyboard is proposed in [10], but numbers are replaced with the images. Results presented in [5,10] shows that visual approaches for user authentication have several advantages over password authentication. The technique proposed in [11] relies on image password which is randomly generated by the system and the authentication process which is based on image recognition. Images that are provided by the user used as "passimages" in [12].

3. HOW GRAPHICAL PASSWORD IS EFFECTIVE?

A graphical password is an authentication system that works by having the user select from images, in a particular order, presented in a graphical user interface (GUI). For the same reason, the graphical-password approach is sometimes termed as graphical user authentication (GUA). A graphical password is much easier than a text-based password for most people to remember. Suppose an 8-character length password is necessary to accesses particular computer network. So, Instead of m8ViI80c, for example, a user might select images of the earth, the country of India (from a map of the world), the city of Ghaziabad (from a map of India), a white colored house with red tiles on the roof, a gray plastic cooler with a black lid, a snap of cheese (some food), a bottle of mango juice, etc.

So, graphical passwords may offer better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words (rather than the recommended complex set of characters). A dictionary search can usually hit on a password and allow a hacker to gain accesses into a system in few seconds. But if a series of some selectable images are used on successive screen pages, and there are many images on each page, a hacker will try every possible combination randomly. And for example, if there are 100 such images on each of the 8 pages in an 8-image password, there are 100^8, or 10 quadrillion (10,000,000,000,000,000), possible combinations that could form our graphical password and if our system has a built-in delay of only 0.1 second (for example) following the selection of each image until the presentation of the next page, it would definitely take (on average) millions of years to break the system by hitting it with random image sequences.

4. TECHNIQUES

There are the two techniques for image based authentication (i) Recognition Based Techniques (ii) Recall Based Techniques

4.1 RECOGNITION BASED TECHNIQUES

The [5] proposed a graphical authentication scheme which is based on the Hash Visualization technique [13]. In that system, the user is asked to select number of images from a set of random pictures generated by a program as shown in figure 1. Afterwards, the user will be required to identify the pre-selected images in order to be authenticated. The results showed that 90% of all participants succeeded in the authentication process using this technique, while only 70% succeeded using text-based passwords. But, the average login time is longer than the traditional approach. A weakness of this system is that the server needs to store the seeds of the images of each user in plain text. Also, the process of selecting the set of pictures from the picture database can be quiet tedious and time consuming for the user.

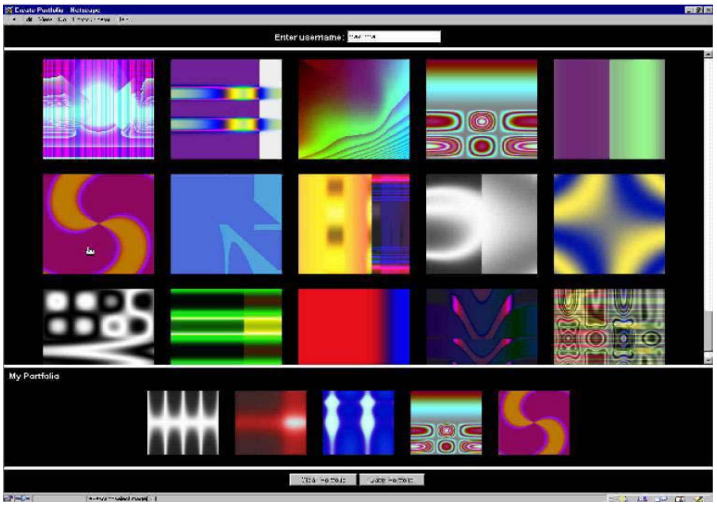

Fig 1.Random images used [5]

One of the algorithms given in [14] is similar to the technique proposed by [5]. The only difference is that the algorithm uses the concept of hash function SHA-1, which produces a 20 byte output, the authentication is secure and requires less memory. The authors suggested a possible future improvement by providing persistent storage and this could be deployed on the Internet, cell phones and PDA's.

When we talk about several authentication schemes as given by [15], which sketched several such schemes, like picture recognition, object recognition and conducted a number of user studies. In the picture recognition study, a user is trained to recognize a large set of images.

Also, [16] developed a graphical password technique that deals with the shoulder surfing problem. In the first scheme, the system will display a number of pass-objects (i.e. pre-selected by user). To be authenticated, a user needs to recognize these pass-objects and click inside the convex hull formed by all these pass-objects shown in figure 2. In order to make

the password difficult to guess, [16] suggested around 1000 objects, which makes the display very crowded and the objects were almost indistinguishable.

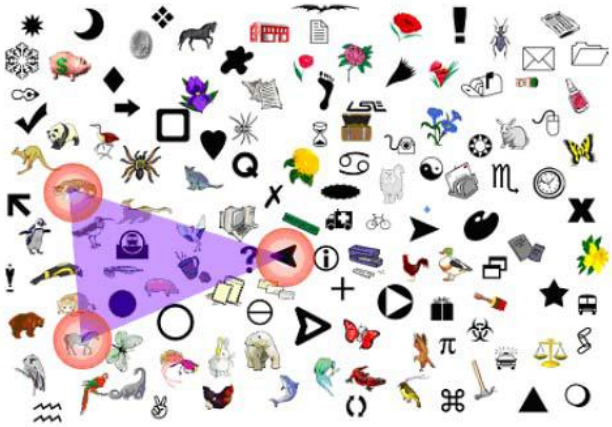

Fig 2.A shoulder-surfing resistant graphical password scheme [16]

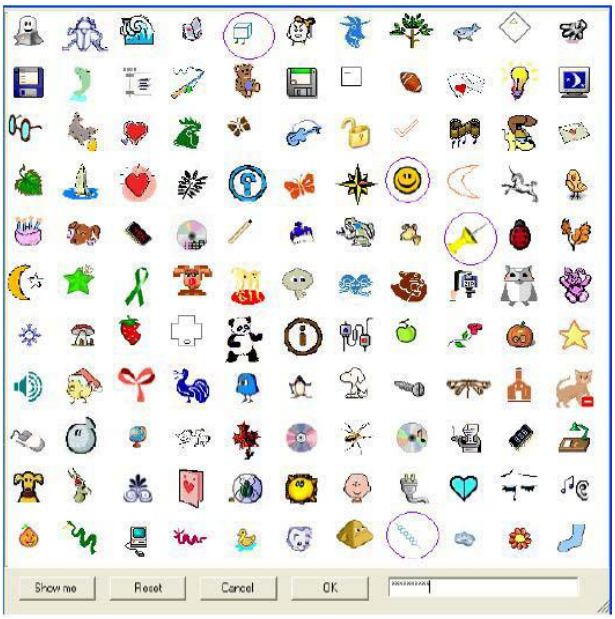

Fig 3.The pass-string is 99dc815lup : shoulder surfing resistant[17]

However, this method also requires users to memorize the alphanumeric code for each and every pass-object variant. Later on [17] extended this approach so that the user will assign their own codes to pass-object variants. Figure 3 shows the login screen of this graphical password scheme.

"Passface" is another technique developed by Real User Corporation [18]. The basic idea is user will be asked to choose four images correspond to human faces from a face database as their future password. In the authentication stage, the user will sees a grid of nine faces and which will consist of one face previously chosen by the user including eight decoy faces (figure 4). Now, the user recognizes and clicks anywhere on the face known to him/her.

This same process is repeated for several rounds. The user is authenticated only if he/she correctly identifies the four faces. This technique is based on the assumption that people can remember and recall human faces easier than any other pictures.

Fig 4.Passfaces [18]

User studies by Valentine given in [19, 20] have shown that Passfaces are very memorable over long intervals. Jansen in [21-23] proposed a graphical password mechanism for the mobile devices.

4.2 RECALL BASED TECHNIQUES

It is a typical implementation which based on the user drawing in a grid canvas. Jermyn in [24] proposed a technique, called "Draw - a - secret (DAS)", which allows the user to draw their unique password, see figure 5.

Currently, too many constraints result in reduction in user experience and prevent its popularity. In this user personalities have a great influence on the drawings and therefore make it harder for others to imitate. Additionally, users can draw the secrets small enough to resist shoulder surfing [5].

Further, in [25] further studied the impact of password length and the stroke-count as a complexity property of the DAS scheme. In the year 2008 [26] described a technique by collecting a corpus of naturalistic description of a set of 45 faces.

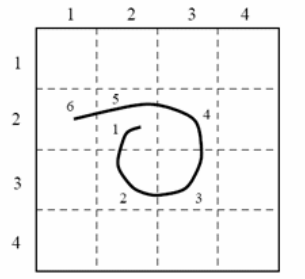

Fig 5.Draw A Secret. [24]

5. Discussion/ How to Apply?

5.1 Is a graphical password as secure as text based password?

A very little research has been done for studying the difficulty of cracking graphical passwords. Since graphical passwords are not widely or commonly used in practice and there is no such report on real cases of breaking graphical passwords. Here we briefly discuss some of the techniques for breaking graphical passwords and will try to do comparison with text-based passwords.

Brute force search: The main defense against brute force search is to have a sufficiently large password space.

Recognition based graphical passwords tend to have smaller password spaces [27-29, 30] than the recall based methods. It is more difficult to carry out a brute force attack against graphical passwords than text-based

Dictionary attacks: The recognition based graphical passwords involves mouse input instead of keyboard input, so it will be impractical to carry out dictionary attacks against this type of graphical passwords[24, 30]. More research is needed in this area.

Guessing: Unfortunately, it seems that graphical passwords may be predictable. More research efforts are needed to understand the nature of these graphical passwords created by real world users.

Spyware: Except for a few exceptions in [17], key logging or key listening spyware cannot be used to break graphical passwords.

Shoulder surfing: Like, text based passwords most of the graphical passwords are seems to be vulnerable to shoulder surfing. None of the recall based techniques are considered shoulder-surfing resistant.

Social engineering: Comparing to text based password, it is less convenient for a user to give away graphical passwords to another person. for example a person cannot give passwords on mobile,

5.2 The Major Points of design issues of graphical password?

5.2.1 Security: In the above section we have discussed security issues.

5.2.2 Usability: A major issue among all the users of graphical passwords is that, the password registration and log-in process takes too long, especially in recognition-based approaches. For example, during the registration stage, a user has to select images from a database of large set of selections. Here in authentication stage, a user has to scan many images to identify a few pass-images. Users may find this process very long and tedious to work on. Because of this and also because most users are not familiar with the graphical passwords, they usually find graphical passwords less convenient than text based passwords.

5.2.3 Reliability: The main design issue for the recall based methods is the reliability and accuracy of user input recognition. In this type of method, error tolerances have to be set carefully.

5.2.4 Storage and Communication: Graphical passwords require much bigger pool of space for storage of images as compared to text based passwords. Here, network transfer delay is also a measure concern, especially for recognition based techniques.

6. Conclusion

The past decade has seen a growing interest in using graphical passwords as an alternative option to the traditional text-based passwords. This paper basically focused on the usability of graphical passwords over the text-based password which seems to hold out the probability of a much more secure system. Here, in this paper, we have conducted a widespread survey of existing graphical password techniques. Although the main argument supporting graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, but the existing user

studies are very limited and there is not yet convincing evidence to support this argument. Overall, we can say that the current graphical password techniques are still immature. Therefore, much more research and user studies are needed for graphical password techniques to achieve higher levels of maturity and usefulness. The main common element of computational trust is user identity. Currently lots of authentication techniques and methods are available but each of these has their own advantages and shortcomings In future, we will plan to investigate the performance issues.

References

[1] A. S. Patrick, A. C. Long, and S. Flinn, "HCI and Security Systems," presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA., 2003.

[2] Wiedenbeck,Waters,Birget,Broditskiy & Memon,2005 "The password problem"

[3] 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.

[4] LinkedIn confirms 'some' passwords leaked By Jaikumar Vijayan in ***Computerworld*** ,June 06, 2012

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

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

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

[8] G. Blonder. Graphical passwords. *United States Patent 5559961*, 1996.

[9] I. Jermyn, A. Mayer, F. Monrose, M.K. Reiter, A. D. Rubin, "The Design and Analysis of Graphical Passwords," *Proceedings of the 8th USENIX Security Symposium*, August, Washington DC, 1999

[10] A.D.Angeli, M.Coutts, L.Coventry, G.I.Johnson, "VIP: a visual approach to user authentication," *Proceedings of the Working Conference on Advanced Visual Interface (AVI2002)*, pp. 316–323, May 2002.

[11] A. Perrig, D. Song, "Hash Visualization: a New Technique to improve Real-World Security," *International Workshop on Cryptographic Techniques and Ecommerce (CrypTEC)*, 1999

[12] T. Taada, H. Koike, "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images," *Proceedings on MobileHCI*, 2003

[13] 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.

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

[15] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in *Proceedings of Conference on Human Factors in Computing Systems (CHI)*. Vienna, Austria: ACM, 2004, pp. 1399-1402.

[16] L. Sobrado and J.-C. Birget, "Graphical passwords," *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*, vol. 4, 2002.

[17] 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*. Las Vergas, NV, 2004.

[18] RealUser, "www.realuser.com," last accessed in June 2005.

[19] T. Valentine, "An evaluation of the Passface personal authentication system," Technical Report, Goldsmiths College, University of London 1998.

[20] T. Valentine, "Memory for Passfaces after a Long Delay," Technical Report, Goldsmiths College, University of London 1999.

[21] W. Jansen, "Authenticating Mobile Device Users Through Image Selection," in *Data Security*, 2004.

[22] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices," National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.

[23] W. A. Jansen, "Authenticating Users on Handheld Devices," in *Proceedings of Canadian Information Technology Security Symposium*, 2003.

[24] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in *Proceedings of the 8th USENIX Security Symposium*, 1999.

[25] J. Thorpe and P. C. v. Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords," in *Proceedings of the 20th AnnualComputer Security Applications Conference*. Tucson, Arizona, 2004.

[26] Paul Dunphy, James Nicholson, Patrick Oliver, "Securing passfaces for description", Proceedings of the 4th symposium on Usable privacy and security, ACM ISBN: 978-1-60558-276-4 2008.

[27] J. Thorpe and P. C. v. Oorschot, "Graphical Dictionaries and the Memorable Space of Graphical Passwords," in *Proceedings of the 13th USENIX Security Symposium*. San Deigo, USA: USENIX, 2004.

[28] J. Thorpe and P. C. v. Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords," in *Proceedings of the 20th Annual Computer Security Applications Conference*. Tucson, Arizona, 2004.

[29] J. Goldberg, J. Hagman, and V. Sazawal, "Doodling Our Way to Better Authentication," presented at Proceedings of Human Factors in Computing Systems (CHI), Minneapolis, Minnesota, USA., 2002.

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

