International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017), e-ISSN: 2455-2585
Volume 4, Issue 6, June-2018

Graphical User Authentication Methods for Enhancing Password Security

Ulya Sabeel

Department of Computer Science and Engineering, Amity University Haryana
usabeel@ggn.amity.edu

Abstract*— The authentication of users is the most critical facet of assuring information security. To safeguard the user and system information from various attacks, password based authentication mechanisms are provided. The most widely used authentication method is using the plain text based passwords. Such passwords may contain a sequence of alphabets, numbers and special symbols. Users mostly choose alphanumeric passwords that are easy for them to recall and many user accounts can have the same password. Such passwords might not be highly secured and may be susceptible to attacks by adversaries. These security vulnerabilities led to the development of graphical passwords as a substitute. Graphical passwords use images in replacement to the alphanumeric characters, which is easier for users to remember and provide better security. This paper focuses on various graphical password techniques, algorithms, their design, implementation and security issues and their comparison based upon security and usability characteristics.

***Keywords*— Authentication, Graphical Password, Password space, Reliability, Security, Usability**

INTRODUCTION

In [1], the authors highlight three major areas (authentication, security operations and developing secure systems) for human computer interaction. For a user to access a network, every web application provides some security mechanism for authentication like providing the username and password. This text based password faces a lot of security loopholes. In addition to this, studies [2] have revealed that users tend to use passwords that are short and easy to remember. This increases the vulnerabilities of text based passwords. The passwords that are difficult to guess by the third party are also difficult to remember. Studies have proved that users often tend to use the same passwords for different accounts and sometimes write them down [3], [4]. To resolve these issues, alternative methods like biometric authentication have been proposed [5], [6].

This paper, however focuses on graphical passwords like pictures for authentication of users. The motivation behind this technique is that users are better in recalling pictures than plain text [7]. The password space for graphical passwords is larger than that of text based passwords, so it is much difficult for the adversaries to crack such passwords. Due to these advantages, graphical passwords are not only becoming increasingly popular for web login applications, but also Internet Banking and ATM applications.

In this paper, an in-depth survey of the existing graphical user authentication techniques has been carried out. The strengths and shortcomings of each method have also been discussed. The rest of the paper has been organized as follows: section II describes related work, section III gives the overview of the authentication methods, section IV describes the graphical authentication algorithms, section V gives major design and implementation issues of graphical passwords, section VI describes the security issues in graphical passwords. Finally, the study is concluded in section VII.

RELATED WORK

Graphical user authentication techniques can be categorized into 3 categories: recognition, recall and cued recall. Among these three, 'Recognition' is the easiest one and 'Pure recall' is the toughest one as the information is accessed from memory without triggers. 'Cued Recall 'comes somewhere in between these two and uses a cue to establish context and trigger stored memory. CCP is one of the existing graphical user technique and is similar in various facets to Passfaces[6], Story and PassPoints[6]. CCP is less complex as compared to Weinshall method [8]. Passfaces primarily deals with recognition of human faces. The user selects few images from a larger set and uses the same set of images already selected by him to login into the account later. For each login, the user is supposed to give a correct response. In [9], the author proposed a graphical password scheme (Faces) based upon Passfaces. The users could accurately remember the images but it became easy to predict resulting in a less secure password. The author then proposed an alternative scheme (Story) that used other general images in replacement to faces and the users had to remember the correct order of images to login into their accounts. Blonder et al. proposed a click based password scheme where the users were supposed to click on specific regions of an image instead of selecting different set of images for each login. Wiedenbeck et al later proposed a technique PassPoints where the user password consists of almost 8 points to be clicked anywhere on the image and each password was converted into a cryptographic key. His experiments revealed that PassPoints could be a usable graphical authentication scheme and was much secure than other methods.

OVERVIEW OF THE AUTHENTICATION METHODS

The authentication techniques can be classified into 3 categories [10]: knowledge based, token based and biometric based. These are represented in figure 1.

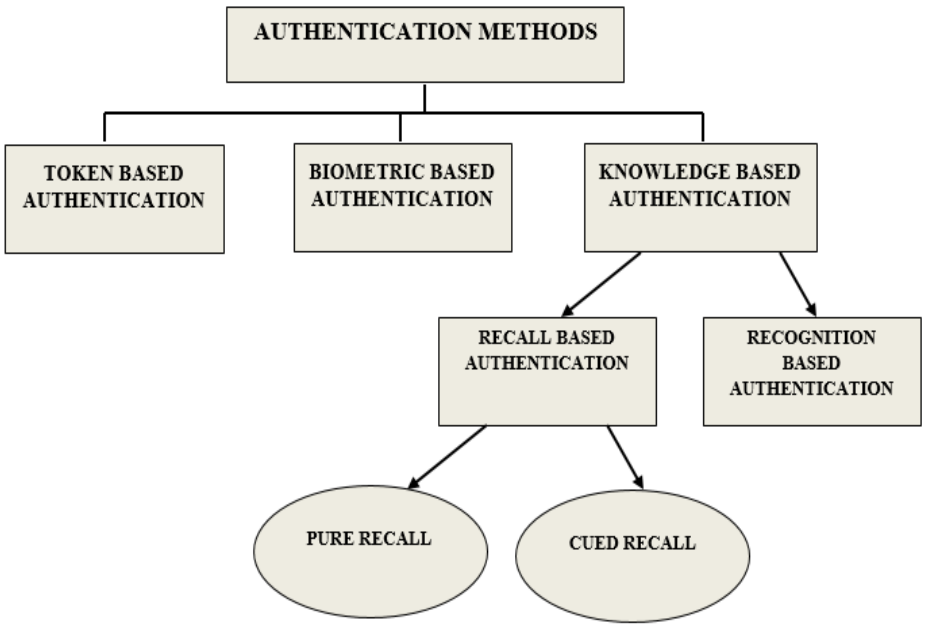

Fig. 1 Authentication methods

Token based authentication:

In these authentication techniques, users are supposed to carry tokens such as key cards, bank cards like an ATM card or other smart cards. Such cards when used, often need a password or PIN number for providing an additional level of security if lost or stolen.

Biometric based authentication:

This type of authentication mechanism is based upon the physical characteristics of users like iris scan, fingerprint scan, palm scan or facial recognition. This method is not so widely adopted because of its expensive nature and slow and unreliable identification process. However, this process provides the highest level of security.

Knowledge based authentication:

These type of authentication techniques are the most commonly used. Such techniques include both text based and picture based passwords. Text based passwords are alphanumeric passwords and picture based passwords are graphical passwords consisting of a series of images to be used as authentication technique for a user. These picture based passwords are further classified into two categories: recognition based and recall based authentication techniques.

1) Recognition based technique:

In this technique, user is provided with an image set and can be authenticated if he correctly identifies the images he selected during the registration phase. Some recognition based algorithms are Déjà vu [11], Hash visualization technique [12], Passface [13].

2) Recall based technique:

In this technique, a user is demanded to produce something that he selected or created during registration phase. Recall based technique is further categorized as pure recall, where the user produces the password without any clue given by the system and cued recall, where the user is given a clue such that he can guess his registered password. Grid selection [15] and DAS [15], are pure recall techniques whereas Blonder [16] and PassPoint [13] are cued recall based techniques.

GRAPHICAL AUTHENTICATION ALGORITHMS

A. *Draw A Secret (DAS) Authentication Algorithm*

This algorithm belongs to pure recall based algorithms in which the user must draw a pattern correctly and no clue is provided by the system. Refer fig 2. The pattern is stored in the form of sequence of coordinates. For successful authentication of the user, he needs to draw the pattern in same manner as was done in the registration process [14]. This technique is mostly used for mobile phone based authentication systems. This system is easy to implement and there is no need to remember difficult alphanumeric passwords. However, if the user is not familiar with this technique, it can prove difficult. Also, the password space is less as compared to alphanumeric passwords.

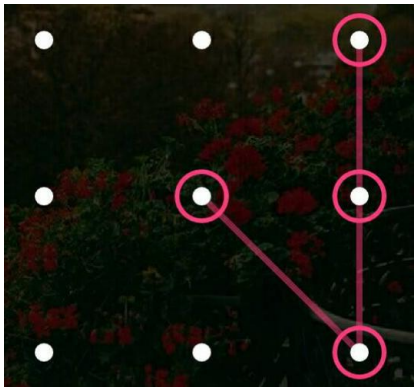

Fig. 2 Draw A Secret

B. *Déjà vu Authentication Algorithm*

This algorithm belongs to the category of recognition based authentication algorithms. Refer fig. 3. The user is given a pool of images generated by Hash visualization technique [12]. During each user registration, a seed value is generated and stored with a trusted third party. The value is then applied to the pixel value to get new images, resulting in a random abstract image output [11]. The technique is easy to execute but time consuming. Also, the seed values stored on the third party might be susceptible to corruption by adversaries, if not secured by a strong security algorithm.

Fig. 3 Déjà vu Authentication Algorithm

C. *Grid selection Authentication Algorithm*

This algorithm belongs to pure recall based authentication algorithms. The user selects a small region from a large grid pattern. This selected region is zoomed on selection [15]. The user then draws a password pattern on this zoomed region as shown in fig 4. This algorithm is better than DAS in terms of password space. The disadvantage of this algorithm is that if the user is not familiar with this technique, it might be difficult for him. Also, recalling of the password pattern might be difficult if the user already selected a difficult pattern during registration.

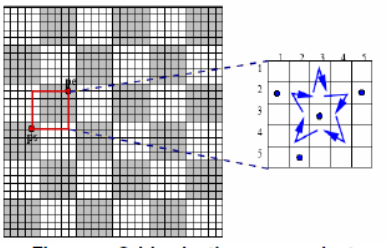

Fig. 4 Grid Selection Authentication Algorithm [15]

D. *PassPoint Authentication Algorithm*

This algorithm belongs to cued recall based authentication algorithms. Here the user can use any image with many possible click points. This image acts as a clue for the user to remember the click points used by the user during the registration process. For successful user authentication, the user needs to select the click points in the same order as done in registration process. There can be an adjustable tolerable distance of 0.25 cm between the actual click points [13]. This is shown in fig 5. Here the user can select as many click points on the image as possible, which makes this technique more secure. The disadvantages of this technique are that this technique is time consuming and click points are difficult to remember.

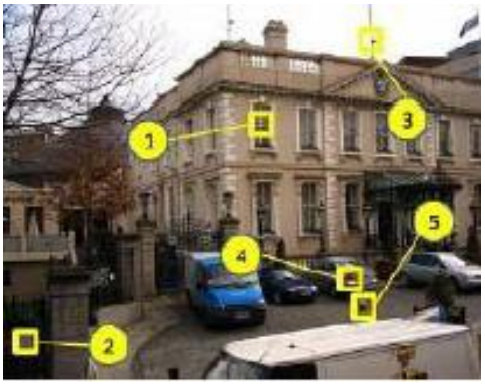

Fig. 5 PassPoint Authentication Algorithm

E. *Usability*

Current studies have revealed that graphical passwords are being used by fewer number of users. A major problem faced by users in using these passwords is the time it takes to login especially in recognition based techniques. The user must pick up a large set of images, or click on many points during the registration process, which makes the process quite cumbersome and time consuming. Therefore, users find graphical passwords less convenient than text based alphanumeric passwords.

F. *Reliability and security*

Reliability and accuracy of user input is a major design problem for recall based authentication schemes. Such a method demands optimal error tolerance mechanisms to avoid false positives or negatives. Also, a more error tolerant system is susceptible to attacks by adversaries. Therefore, it is highly required to improve the error tolerance in such systems. The security issues of graphical passwords have been mentioned in the next section.

G. *Storage and Communication*

The requirement of storage space in graphical passwords is high as compared to text based passwords. The pictures selected by the user or the or the seed values generated from user click points need a centralized and secure database for storage. The communication delay is another problem associated with graphical passwords. For authentication of the user, many images need to be displayed for different phases of verification.

II. SECURITY ISSUES IN GRAPHICAL PASSWORDS

Graphical passwords are not widely used but still might be susceptible to some security vulnerabilities. The security attacks possible in these passwords are less as compared to text based passwords. Some of them have been mentioned here.

A. *Brute Force Attack*

In such an attack, exhaustive key search is done and every possible combination is taken to hack the password until it is finally cracked. To defend the user from such an attack, a considerably large password space is needed. The text based passwords have a password space of 94^N, N being the password length and 94 is the number of printable characters not including space. The textual passwords are more vulnerable to such an attack as compared to graphical passwords where it is quite difficult to mimic the actual mouse motion or other human input.

B. *Dictionary Attack*

This attack involves a comprehensive list of words that are most likely selected by the users as their passwords. Since graphical passwords are mostly based upon mouse inputs rather than keyboard inputs, they are very difficult to crack as compared to text based passwords. In some recall based authentication methods, automated dictionary based attacks are possible but is much more complex than text based passwords [14], [18]. Overall, graphical passwords are less vulnerable to dictionary attacks as compared to alphanumeric text based passwords.

C. *Guessing*

The graphical passwords are often quite foreseeable and have less password space than text based passwords. In Passface technique [9], the authors have shown that users tend to choose easy and predictable graphical passwords. Some more research needs to be done to understand the nature of such graphical based passwords.

D. *Spyware Attack*

This kind of attack involves the adversary's software to be installed on the user's system without him knowing and recording the user's each keystroke and mouse click. The movement of the mouse is not enough to break graphical passwords, it needs to be correlated to the exact coordinates too. Further research needs to be done to make it clear whether such types of attacks can be launched effectively on graphical passwords.

E. *Shoulder surfing Attack*

This kind of attack is carried out by the adversary by looking over the user's shoulder when the user is entering his password. This is more common in places like offices, markets, public places like ATMs and other crowded places. Most of the graphical as well as text based passwords are susceptible to these attacks. Some recognition based graphical passwords are designed to resist such attacks [20], [21]. None of the recall based authentication methods are found to be shoulder surfing resistant yet.

F. *Social Engineering Attack*

This attack deals with manipulating the users into performing such activities which reveals their confidential information like bank passwords and account details. As compared to text based passwords, graphical passwords are difficult to reveal to other people and it is very time consuming and tedious to launch phishing attacks to gain access to a user's graphical password. Therefore, it is difficult to break graphical passwords as compared to text based using this method.

There is a requirement for more exhaustive research methods that enquire the possible attack against graphical authentication passwords. Table 1 gives the comparison of graphical authentication algorithms based upon the security issues. Table 2 depicts the comparison of graphical authentication algorithms based upon their usability characteristics.

TABLE I
COMPARISON OF GRAPHICAL AUTHENTICATION ALGORITHMS BASED UPON SECURITY ISSUES

S.No.	Graphical Authentication Algorithms	Security Attacks					
		Brute Force	Dictionary	Guessing	Spyware	Shoulder surfing	Social Engineering
1	DAS				✓	✓	
2	Deja Vu	✓	✓				✓
3	Grid selection				✓		
4	PassPoint				✓	✓	

TABLE II
COMPARISON OF GRAPHICAL AUTHENTICATION ALGORITHMS BASED UPON USABILITY CHARACTERISTICS

S.No	Graphical Authentication Algorithms	Usability Characteristics		
		User Friendliness	Reliability	Accuracy
1	DAS	✓	✓	✓
2	Deja Vu		✓	✓
3	Grid selection	✓	✓	✓
4	PassPoint		✓	

CONCLUSION

In the recent years, there has been a burgeoning interest in using graphical passwords as a replacement to traditional alphanumeric passwords. In this paper, an in-depth study of the most popular graphical password techniques has been carried out. These techniques have been categorized as recognition based and recall based. In addition to this, the design, implementation and security issues of these techniques have also been mentioned. The survey suggests that the graphical authentication based passwords are difficult to crack using traditional attack methods like brute force, spyware attack or dictionary based attacks in comparison to the traditional text based passwords. These graphical passwords are not that widely used due to their usability, reliability and storage based issues and their security issues are still not well understood. Comprehensive research and an in-depth study is needed for these graphical user authentication methods to achieve higher levels of usefulness and widespread adoption within our authentication systems.

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

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

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

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

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

[8]. D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing

[9] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proceedings of the 13th Usenix Security Symposium. San Diego, CA, 2004.

[10] Information Security Principles and Practice by Mark Stamp - Second Edition.

[11] Rachna Dhamija, Adrian Perrig, "Déjà Vu: A User Study. Using Images for Authentication", in the proceeding of the 9th USENIX security Symposium, 2000.

[12] Rachna Dhamija, "Hash visualization in user authentication", Proceedings of CHI 2000 ACM, The Hague, the Netherlands.

[13] Susan Wiedenbeck, Jim Watersa, Jean-Camille Birgetb, Alex Brodskiyc, Nasir Memon;, "Design and longitudinal evaluation of a graphical password system", Academic Press, Inc. 102-127, 2005

[14] Jermyn Ian, A. Mayer, F. Monrose, M. K. Reiter, A. D. Rubin, "The design and analysis of graphical passwords", Proceedings of the Eighth USENIX Security Symposium, USENIX Association 1–14, 1999.

[15] J. Thorpe and P. C. v. Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords," in 20th Annual Computer Security Applications Conference (ACSAC) Tueson, USA. IEEE, 2004.

[16] Blonder, G. E. Graphical Passwords, Murray Hill, NJ, US Patent, 1996

[17] Muhammad Daniel Hafiz, Abdul Hanan Abdullah, Norafida Ithnin, Hazinah K. Mammi, "Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique"; IEEE Explore, 2008.

[18] 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.

[19] D. Nali and J. Thorpe, "Analyzing User Choice in Graphical Passwords," Technical Report, School of Information Technology and Engineering, University of Ottawa, Canada May 27 2004.

[20] 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.

[21] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in *Proceedings of International conference on security and management*. Las Vegas, NV, 2003.