International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Research Article

A Recognization Based Graphical Password System

Nilesh Kawale[Å*] and Shubhangi Patil [Å]

[Å]Computer Science & Engineering, R.T.M.N.U, India

Accepted 01 April 2014, Available online 10 April 2014, **Vol.4, No.2 (April 2014)**

Abstract

The most important thing in the network security is to provide user authentication. Therefore passwords are used in the vast majority of computers and communication systems for authentication. Passwords may be of two types, text based password and Graphical password. Using Text Based strong passwords, provides good security but memorizing text based password is so difficult. In such case, users have to write it on piece of paper or have to save inside computer. This paper provides an alternative solution to text based password authentication which is Graphical Password. Graphical password approach is also known as Graphical Password Authentication (GUA). Graphical password is much easier and simple to remember than text based password. This type of interface provides better way to remember images better. However, issue with GUA is shoulder surfing attack which can capture users mouse clicks. In this paper, we will propose to reduce the shoulder surfing attack up to certain extend with the random character set generation for each image using the concept of watermarking.

Keywords: *Graphical Password, Shoulder Surfing, Authentication Security, Alphanumeric Password.*

1. Introduction

In modern communication networks, a user can easily and conveniently obtain wanted resources. A user sends the request and authenticated to obtain the server's resources anytime and anywhere. In order to ensure only legal users can obtain the service, many user authentication schemes have been proposed. With password, authentication is common approach because passwords are easy to remember.

Mainly the problem arises because passwords are expected to comply with two fundamentally conflicting requirements:

1. Password should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans.
2. Password should be secure i.e. they should look random and should be hard to guess; they should be changed frequently and should be different accounts of the same user; they should not be written down or stored in plain text.

Users need to prove they are who they claim to be for many services, such as online banking, e-mail and e-commerce. Currently, alphanumerical passwords are the authentication mechanism of choice. However, passwords have a number of well documented problems associated with them, such as use of weak passwords and lack of memorability. Memorability has two perspectives:

1. The process of selecting and the encoding of the password by the user.
2. Defining the task that user has to undertake to retrieve the password.

Therefore an alternative to this problem, a graphical authentication mechanism is used in which user is asked to select an image, points on image or draw an image in order to authentic. Such schemes are separated in to three categories: recognition-based, recall-based, and cued-recall.

This work concerned with recognition-based scheme. In this user selects number of images from Given Image set. In order to authenticate, user must then select their images from the image set.

2. Related work

2.1 Problems with Alphanumeric Password

Mainly the password problem arises from limitation of humans Long Term Memory. Once the password has been chosen and learned the user must be able to recall it to log in. But usually people forget the password. Many items in memory may compete with a password and prevent its accurate recall. If a person fails to use password for long time, it will be even more susceptible to forgetting. A further problem is that users have many passwords for computers, networks, and web sites. The large number of passwords increases interference and is likely to lead to forgetting or confusing passwords.

Users typically cope with the password problem by decreasing their memory load at the expense of security. First, they write down their passwords. Second, when they

*Corresponding author: **Nilesh Kawale**

have multiple passwords, they use one password for all systems or trivial variations of a single password.

2.1 Graphical Password

Most of the graphical password systems are based on either recognition or cued recall. In recognition-based system the user must recognize previously chosen images from the larger group of distractor images. In cued recall password system user must click on several previously chosen areas in an image, cued by viewing the image.

Both types of system may have memory advantages over alphanumeric password. Alphanumeric passwords are totally based on pure recall. It is known that recognition memory is better than unaided recall. Furthermore, psychological studies show that images are recognized with very high accuracy after 2 hours delay, which is much higher than accuracy for words and sentences. Studies of recall also confirm that pictures are recalled well than words and this has led to the tag picture superiority effect.

Efficiency is important in password system because user wants to have quick access to system. The time to input a graphical password by a highly skilled, automated user can be predicted by Fitt's Law. The law states that the time to point to a target depends on the distance and size of target- greater distance and smaller target lead result in slower performance. Graphical Authentication Techniques are categorized into three groups:

1) Pure Recall Based: In this system Users reproduce their passwords, without having the chance to use the reminder marks of system. Although easy and convenient, it appears that users do not quite remember their passwords.

2) Cued Recall Based: Here, the system provides a framework of reminders, hints and gestures for the users to reproduce their passwords or make a reproduction that would be much more accurate.

3) Recognition Based: Here, users select pictures, icons or symbols from a bank of images. During the authentication process, the users have to recognize their registration choice from a grid of image. Research has shown that 90% of users can remember their password after one or two months

.

3. Graphical Password Attack

1) Brute Force Attack: This type of attack produces every possible combination of words to break the password. This type of attack has always proven successful against text-based password because of its ability to check all possibility within the length of the password. Therefore, users are advised to select a stronger and complex password to prevent discovery from brute force attack. However, GUA proves to be more resistant to brute force attacks since the attack software needs to produce all possible mouse motions to imitate passwords especially when trying to recall the graphical passwords.

2) Dictionary Attack: This type of attack uses words found in the dictionary to check if any were used as passwords by the users. Many users' uses weak passwords which make it easier for attackers to guess the password using the graphical dictionary attack. Because of graphical password method of using mouse input type recognition, using dictionary attack on GUA would be a waste of time.

3) Spyware Attack: This attack uses a small application installed (secretly) on a user's computer to record sensitive data during mouse movement or key press. This form of malware secretly store these information and then reports back to the attackers system. With a few exceptions, these key-loggers and listening spywares are unproven in identifying mouse movement to crack graphical passwords.

4) Shoulder Surfing Attack: As the name suggests, passwords can be identified by looking over a person's shoulder. This kind of attack is more common in crowded areas where it is not uncommon for people to stand behind another queuing at ATM machines. There are also cases where ceiling and wall cameras placed near ATM machines are used to record keyed pin numbers. The best way to avoid pin numbers being recorded or remembered by attackers is to properly shield the keypad when entering the pin number.

5) Social Engineering Attack (Description Attack): This type of attack happens when a non-authorized personal manages to impersonate authorized employees and access confidential information (i.e.) passwords and codes. The attacker interacts with unsuspecting employees and gathers as much information they can to gain access to the protected data. The process is repeated until the correct identity is obtained.

6) Physical Attack: This type of attack happens when a user can access directly to the data in the server. It makes a chance for attacker to bypass the authentication process and directly access to the resources. In graphical password by physical attack is possible to access the image gallery and password database. If attacker access to the image gallery then it is possible to change the images and make a miss functioning for the system in next login and registration processes. And if attacker access to the password database then it is possible to login to the system by any user name.

4. Proposed Graphical Password System

4.1 Registration Phase: The diagram below shows the registration phase of the system. The image matrix contains the password. User can select some images from the matrix as password and submit to the system. For example, in the image below user selects three images as the password.

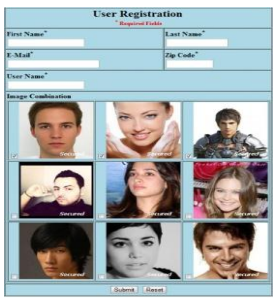

Fig. 1 Registration Phase

4.2 Login Phase: In login phase, user must have to enter user id, entered during registration phase and password, obtained on mobile and have to select same three images that were selected during registration phase. This process is used to secure the login process from shoulder surfing attack while keeping it simple for users without having to memorize complex passwords.

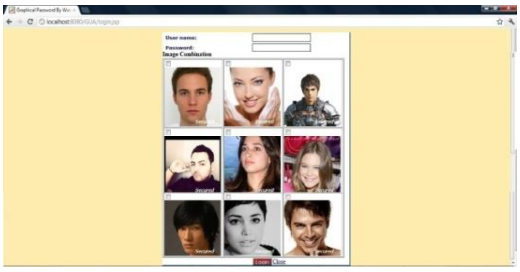

Fig. 2 Login Phase

As the user entered the password, it will get match with the database password; stored during registration phase. Once match is found to be true, it (user entered password) will again matches with number generated due to selection of images. As match is found to be true then user can login to system. That means user will get the access only when entered password and selected images are matches.

4. Proposed System Evaluation

We will discuss about all probable attacks on our proposed system

1) Brute Force Attack: If we consider brute force attack, then it is advisable to user large password. Therefore one way of reducing and resisting brute force attack: have unfixed number of images that can selected as password and randomly generate number for each image as a password during registration phase to minimize any chance of password being discovered.
2) Dictionary Attack: This method of attack means that the attacker needs a dictionary of all images stored but our system generating random number for images all the time then it will be difficult for any attempt to happen.
3) Spyware Attack: Random images that were generated by the system helps prevent any spyware, malware or any other capturing software to record password via keyboard or mouse. It is almost impossible to match the correct characters and images to capture it.
4) Shoulder Surfing Attack: Here both mouse and keyboard are used to provide and stronger form of security so that no one can immediately guess the password or pin. The only problem with this method is the use of CCTV to record the mouse and keyboard input of each user thus allowing better chance of guessing the code.
5) Social Engineering Attack (Description Attack): This kind of attack is inappropriate since it directly deals with certified user being imitated and not the system.

Conclusions

It has been observed that people tends to remind the combination of geometrical shapes, patterns, colors and texture better than alphanumeric character that are meaningless to user. Therefore this shows that graphical password is more desirable alternative to alphanumeric password. In this paper we focus on attacks of graphical password. This paper proposes a new graphical password system that uses a random character set to provide a stronger security against image gallery attack and shoulder surfing attack.

References

A.H. Lashkari, F.T., Graphical User Authentication (GUA). 2010: Lambert Academic Publisher.

Komanduri, S. and D.R. Hutchings (2008), Order and Entropy in Picture Passwords, in Canadian Information Processing Society.

L.Backerud, K.Nilsson, N.Steen,(1975) The metallurgy of cast iron,St.Saphorin,SwiitzerlandGenrgi publishing company,pp.625-637.

Hu, W., X. Wu, and G. Wei (2010), The Security Analysis of Graphical Passwords, in International Conference on Communications and Intelligence Information Security.

Lashkari A.H., A.G., Leila Ghasemi Sabet, Samaneh Farmand (2010), A New Algorithm on Graphical User Authentication (GUA) Based on Multi-line Grid. Scientific Research and Essays (SRE).

Hayashi, E. and N. Christin (2008), Use Your Illusion: Secure Authentication Usable Anywhere, in Proceedings of the 4th symposium on Usable privacy and security (SOUPS). ACM.

Chiasson, S., et al. (2009), Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords. ACM.

Wiedenbeck, S., J.-C. Birget, and A. Brodskiy (2005), Authentication using Graphical Passwords:Effects of Tolerance and Image Choice, in Symposium on Usable Privacy and Security (SOUPS).

Dhamija, R. and A. Perrig, D´ej`a Vu (2000): A User Study. Using Images for Authentication, in The proceeding of the 9th USENIX security Symposium. USENIX

Man, S., et al. (2004), A password scheme strongly resistant to spyware, in Int. Conf. on Security and Management.Las Vegas.

Forget, A., S. Chiasson, and R. Biddle (2010), Shoulder-Surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords. ACM.

Lashkari A.H., S.F., Omar Bin Zakaria and Rosli Saleh (2009), Shoulder Surfing attack in graphical password authentication. International Journal of Computer Science and Information Security (IJCSIS).

Man, S., D. Hong, and M. Matthews (2003), A Shoulder-Surfing Resistant Graphical Password Scheme – WIW, in International conference on security and management.: Las Vegas.

CAPEC, Standard Abstraction Attack Pattern List (Release 1.6). 2011, Common Attack Patterns Enumeration and Classification (CAPEC): USA.

Todorov, D. (2007), Mechanics of User Identification and Authentication: Auerbach Publications.

Gordon, P. (2007), Data Leakage - Threats and Mitigation, in InfoSec Reading Room. SANS Institute.

Kumar, V., et al. (2009), Click to Zoom-inside Graphical Authentication, in International Conference on Digital Image Processing. IEEE

Dunphy, P. and J. Yan (2007), Do Background Images Improve Draw a Secret Graphical Passwords?, in Proceedings of the 14th ACM conference on Computer and communications security.ACM: Alexandria, Virginia, USA.

Tang, Q. and K.-K.R. Choo (2006), Secure Password-based Authenticated Group Key Agreement for Data-Sharing Peerto-Peer Networks, in Proceedings 4th International Conference on Applied Cryptography and Network Security (ACNS'06). Springer: Singapore.

Hafiz, M.D., et al. (2008), Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique. IEEE.

Wiedenbeck, S., et al.(2005), Design and longitudinal evaluation of a graphical password system. Academic Press, Inc. 102-127.

Li, Z., et al. (2005), An Association-Based Graphical Password Design Resistant To Shoulder-Surfing Attack, in IEEE. University of Cagliari, Italy.

Suo, X., Y. Zhu, and G.S. Owen (2005), Graphical Passwords: A Survey, in Proceedings of the 21st Annual Computer Security Applications. IEEE.

Zheng-ding, L.T.Q. (2002), The Survey of Digital Watermarkingbased Image Authentication Techniques, in IEEE, ICSPOP Proceedings.

Zheng, D., Y. Liu, and J. Zhao (May 2006), A Survey of RST Invariant Image Watermarking Algorithms, in IEEE CCECE/CCGEI, Ottawa.