IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

‘Advanced Security Primitive Using Digital Images’

Abheesh Dokras[1], Chetan Dhapure[2], Akshay Dang[3], Jayesh Kawale[4]

Department of Computer Technology, Priyadarshini Institute of Engineering & Technology, Nagpur (MS), India[1,2,3,4]

Abstract: There are several texts based and graphical password techniques based which are being used for user authentication. In current scenario many of the applications being developed for user authentication are text based password. Text passwords are comparably not secured as the graphical passwords because text passwords easily suffer from man attacks like shoulder suffering, dictionary attacks and many more. They can be easily breached with number of different techniques. The textual passwords will be either alphabetic, numeric or alphanumeric type (i.e. combination of alphabets as well as numbers and special characters). The research shows that text passwords are complex and hard to remember and hence humans select a short password which is simple in some manner to memorize and recall. As a result the security is not so accurate in the present scenario. In our system we are proposing the enhanced security by Captcha technology in which the images are fixed and the texts called Captcha are changed every time and hence it is more secure than traditional technique. By using graphical password system and Captcha technology a new security primitive will be introduced. In this system the watermarking method will be used in database to hide the actual images by simple codes. Working of the system will be done through, user need to register first and then selects number of images as a password after that while login user needs to enter the random code generated by the previously selected images as password an access his account by this system. In a case, if user forgets the password then user will be able to recover the account by a secure provision. And hence the security will increase automatically than traditional password entering techniques because user need to enter different set of codes every time while login. It means there is no need to remember the complex and difficult textual passwords. Instead of that user need to just identify the image and enter the codes below that image. By this technique we will try to upgrade to the existing security for better and secure password based systems.

Keywords: Authentication, Captcha, Digital Images, Graphical password, Watermarking.

I. INTRODUCTION

In generally the password authentication is the most common method to access control for particular operation. Every user has to enter sequence of characters commonly referred to as a password or authentication system. For accessing the operations one must providing the right password. In this scenario textual password is the most common approach for authentication. Whereas password authentication system will encourage strong passwords while maintaining memorability .And therefore length & random passwords can make the system secure in all way. Research studies shown that most of the users tend to pick simple passwords or those that are easy to recall. But unfortunately, passwords can be easily guessed or cracked by using some algorithm. This will be vulnerable to eves dropping, dictionary attack, social engineering and shoulder surfing etc. Common attack for breaking password authenticated systems is dictionary attack [1]. As per a Computerworld news article, one of the expert security team in company ran a network password cracker and within some seconds, they cracked about 80% of the passwords in a stroke .This can be result as if any system is provided with user friendly authentication it becomes easy to break and use that system.

As per the problem situation we are focusing on another alternative that is by using pictures as passwords. Graphical password schemes are the perfect alternative to text-based schemes for security purposes motivated by the fact that pictures can be better remembered by human. And thus graphical password method is more secure than traditional method and can be categories as Recognition Based Techniques and Recall Based Techniques.

Psychological studies have proved that the humans are better at recognizing and recalling pictures than text. As per some research by Patrick, et al. they pointed out that developing secure systems, authentication and security operations are some major areas where human computer interaction is valued. In this system we are using Captcha technology, basically Captcha (Completely Automated Public Turing tests to tell Computers and Humans Apart) is a program that generates a random runtime code that are understandable by humans and not by computer programs because they do not have ability to solve.

The Captcha is the technology which is used by many important services like email, online polls, search engine bots and others. Captcha provide a puzzle that are easy to understand the humans and difficult for the computer programs to handle puzzle beyond capability of computers. Preventing dictionary attacks, worms and spam [2].Captcha is now a standard Internet security technique to protect online email and other services from being abused by bots protection against online dictionary attacks on passwords this threat is widespread and considered as a top cyber security risk [3].

DOI 10.17148/IJARCCE.2016.5174

II. BACKGROUND

A. Attacks on password

The researcher has been done lots of research to study the several numbers of attacks on passwords. Because in today's modern days graphical passwords will not popularly in used, here we proposing there are numbers of techniques that will be used to crack the passwords and we will try to do comparison with the text-based passwords.

1) Dictionary attacks

In graphical password which is based on recognition will get the input from mouse instead of keyboard, this will be very difficult to carry out dictionary attacks against such type of the graphical passwords. For some mesmerize based Graphical passwords, it will be easy to use a dictionary attack but a text based dictionary attack is not complex then the automated dictionary attack. In computer security, a dictionary attack is a technique for defeating a authentication mechanism by trying to determine its decryption key or passphrase by trying hundreds or sometimes millions of likely possibilities, such as words in a dictionary.

2) Shoulder Surfing

Shoulder surfing is vulnerable to the most of the password like text based passwords. At this point, only a few recognition-based techniques are designed to resist shoulder-surfing. None of the recall based techniques are considered should-surfing resistant.

3) Social Engineering

Social Engineering is a less convenient than the text based password. Social Engineering is less convenient for the user to give the graphical passwords to another person. E.g. it will be difficult to give away graphical passwords over the phone. To obtain graphical passwords by phishing web site would more time consuming techniques. However we considered that the breaking graphical passwords will be very difficult using thetraditionalattack techniques like spyware, brute forceattack anddictionary attacks. There is a need for more in-depth research that investigates possible attack methods against graphical passwords.

4) Guessing

It has been a very difficult task to predict what exactly the graphical password is major problem associated with text-based passwords. For example, studies on the Pass faces technique result that the peoples always predictable and a weak graphical passwords. Password guessing is an attack in which an attacker attempts to recover user credentials through the process of attempting to log in repeatedly. This is generally done by using commonly used or default passwords—attempting every possible combination until successful. Password guessing can be used to attack multiple types of systems.

B. Watermarking

Originally a watermark is a more or less transparent image or text that has been applied to a piece of paper, another image to either protect the original image. A transparent watermark is added to a photo by changing the image on the pixel level. The pixels that will make up the resulting watermark is changed more or less in the direction of the watermarking image There is done a lot of research into adding an invisible watermark to images that is hard to remove again. The correlation measure compares the extracted with the original watermark and a statistic of the correlation process is produce to ensure the existence of the watermark [5].

III. EXISTING SYSTEM

The current authentication scheme can be into several major schemethat are as

A. Text Based Password

Text based password can contain characters, numbers, alphanumeric, special characters. People are generally used the text password that is easy to remember but this password are less vulnerable and easy to crack. Text based password can be guess by the number of attacks like brute force, shoulder surfing etc. So the text based password scheme has failed. Therefore the new password scheme has been developed which is based on graphical password.

B. Graphical Password

In Graphical password scheme, User has a combination of images or the set of images, which can use those images as a password. The graphical passwords are easy to remember and hard to guess. The graphical password scheme have minimizes the chances of attacks like brute force and shoulder surfing. Dhamija and Perrig proposed a graphical authentication scheme where the user has to identify the pre-defined images to prove user's authenticity [7]. In this system, the User selects a certain number of images from a set of random pictures during registration.Later, duringlogin the user has to identify the pre-selected images for authentication from a set of images as shown in figure 1.

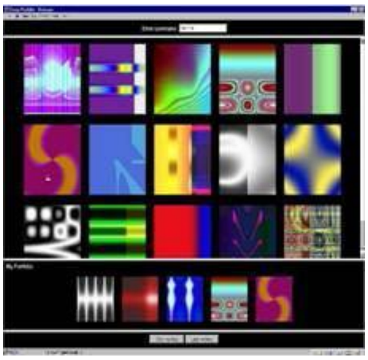
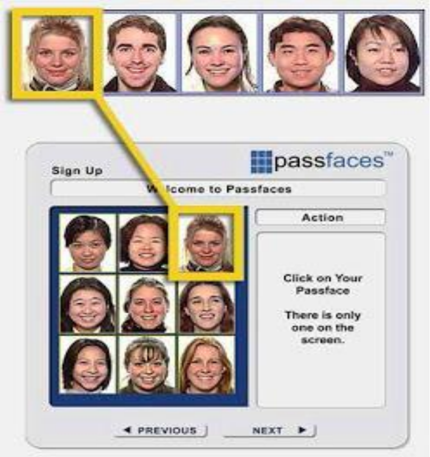


Fig 1: Example of Graphical Password

C. Passface

This is a technique where the user sees a grid of nine faces and selects one face as password from previously chosen by the user as shown in figure 2. Here, the user chooses four images of human faces as their password and the users have to select their pass image from eight other decoy images. Since there are four user selected images it is done for four times. [8]

DOI 10.17148/IJARCCE.2016.5174



Click on Your Passface

There is only one on the screen.

Fig 2: Example of Passface method

IV. CONCLUSION

In this paper we proposed that an authentication is an essential component in most of the security contexts. We try to provide an effective graphical password authentication system with the help of Captcha that will deliver more security than traditional password entering technique. Research's show that user authentication is the most valuable term in respect to information security. And hence this proves that graphical password is a perfect alternative over text based passwords. By this system we will try to provide security in which random set of

Characters that will be generated on runtime with the help of Captcha for stronger security. This paper covers an important term in security i.e. CAPTCHA as Graphical Password schemes. As per the security, usability and practical applications, graphical password using Captcha technology have an effective terminology. In this paper we also introduce watermarking technique for more safe and secure atmosphere. With the help of this system user will be able to secure all his online accounts by simply one security primitive. Users will not need to remember his entire textual password or any other term. He just needs to keep his set of images that provides access to accounts. And thus we try to evaluate a working system for securing the web account access with great extent.

REFERENCES

[1] Matthew Dailey, Chanathip Namprempre, "A Text-Graphics Character CAPTCHA for Password Authentication"

[2] Liming Wang, Xiuling Chang, ZhongjieRen, HaichangGao, Xiyang Liu, UweAickelin, "Against Spyware Using CAPTCHA in Graphical Password Scheme"

[3] HP TippingPointDVLabs, Vienna, Austria. (2010). Top Cyber Security Risks Report, SANS Institute and Qualys Research Labs [Online].

[4] Zheng-ding, L.T.Q., the Survey of Digital Watermarking based Image Authentication Techniques, in IEEE, ICSPOP Proceedings.2002.

[5] Luis P´erez-Freire, P.C.n., Juan Ram´onTroncoso-Pastoriza, and Fernando P´erez-Gonz´ale, Watermarking Security: A Survey. Springer-Verlag Berlin Heidelberg, 2006.

[6] T. S. Ravi Kiran, Y. Rama Krishna, "Combining CAPTCHA and graphical passwords for user authentication", International Journal of Research in IT & Management, Volume 2, Issue 4 (April 2012) (ISSN 2231-4334)

[7] R.Dhamija and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.

[8] Real User Corporation: Passfaces. www.passfaces.com

[9] K. Golofit. Click password under investigation. 12th European Symposium on Research in Computer Security, LNCS 4734, Sept 2007.

[10] Bin B. Zhu, Jeff Yan, GuanboBao, Maowei Yang, and NingXu,"CAPTCHA as Graphical Passwords—A New Security Primitive Based on Hard AI Problems", IEEE TRANSACTIONS ONINFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 6, JUNE 2014

[11] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe. Purely automated attacks on passpoints-style graphical password. IEEEE Trans. Info. Forensics and security, vol. 5, no. 3, pp. 393-405, 2011

[12] HaichangGao, ZhongjieRen, Xiuling Chang, Xiyang Liu UweAickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing"

[13] Alankrita Ladage, Swapnil Gaikwad, Prof. A. B. Chougule. Graphical Based Password Authentication. International Journal of Engineering and Technology, vol. 2, Issue 4, April 2013.