IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

Graphical Password for Desktop

Rashmi Thawani[1], Priyanka Rao[1], Aditi Jadhav[1], Soniya Rajgire[1]

Student, IT, Rajarshi Shahu College of Engineering, Pune, India[1]

Abstract: Today Information Technology has gained momentum in our day today life. Information Technology means use of computers and internet to store and manipulate the information. So all the organizations, industries and also every individual are using computers to store and share or communicate the information. So here security is much important while storing and communicating the information over internet or through computer and its devices to avoid unauthorized access. For this security various techniques are available. Among them the most common and easy to use is a password. For security purpose every application provides user authentication. From ancient days, secret data or code is used for hiding and this gives security to information. Most traditional approach is in which we have to pass through username and password. Authentication process is divided into Token based authentication Biometric based authentication and Knowledge based authentication. Many web applications provide Knowledge based authentication which includes alphanumeric password and graphical password as well. In today's changing world when we are having number of networks and personal account some sort of easy authentication schema needs to be provided.

Keywords: Password, Graphical password, alphanumeric password, security primitive.

I. INTRODUCTION

The information stored by the computer systems are valuable resources which need to be protected. Password can be easily cracked by using practices like online guessing attack, online dictionary attack and shoulder surfing attacks. Due to such attacks a big question on the security system arises. We refer to the security and usability problems associated with alphanumeric passwords. The problem arises because passwords are expected to include two conflicting requirements: 1) Passwords should be easy and memorable, 2) Passwords should be secure, i.e. they should be hard to guess, also they should be changed frequently and should be different on different accounts of the same user, should not be written down or stored. Satisfying these requirements is highly impossible for users. Users often end up ignoring the requirements, which leads to poor password practices.

This problem has led to innovations to improve passwords. Standard internet security technique recently used is graphical password, i.e., passwords that are based on images rather than alphanumeric text. The idea is to use images which will be easy to memorize and will decrease the tendency to choose insecure passwords. This will increase overall password security. The main motto is to provide user with dynamic password approach and increase memorability.

II. OVERVIEWOF THE AUTHENTICA-TION METHODS

Current authentication methods can be divided into three main areas:

- Token based authentication
- Biometric based authentication
- Knowledge based authentication

Token based authentication-
Techniques such as 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 scanner or facial recognition systems are not yet widely adopted because such systems can be expensive and the identification process can be slow and often unreliable. But, this type of technique provides the highest level of security.

Knowledge based authentication-
Techniques are the most widely used authentication techniques which include text-based and picture-based passwords. The picture-based techniques is further divided into two categories: recognition-based and recall-based graphical techniques.

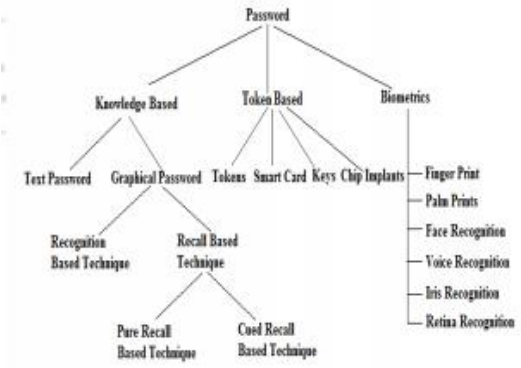

Figure 1: Classification of Password Authentication Techniques

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

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.

III. EXISTING WORK

A. Graphical Password

The requirement for graphical password is that graphical passwords are easier to recall, where we have to write less and have the potential to provide a good symbol space. Many approaches have been proposed in present times. The initial idea of graphical password was given by Blonder in 1996[10]. In his scheme, one predetermined image is presented to a user on a visual display and need to select one or more predetermined positions on the displayed image in an order to access the restricted resource [1]. The drawback of this scheme is that users will not be able to click arbitrarily on the background. The author either dint study the memorable password space.

Sonia Chiasson et al. [2] proposed Cued Click Points (CCP), a cued-recall graphical password technique. In this a password consists of one click-point for every image for a sequence of 5 images. Based on the previous click-point the another image gets displayed and users receive quick feedback whether they are on the correct path when logging in. A wrong click leads down to an incorrect path with an indication of authentication failure only after the final click. The time when they see a wrong image, they know that the recent click-point was wrong and can terminate this attempt and try again from the beginning.

Dhamija and Perrig [3] proposed a graphical authentication scheme in which a certain number of images from a set of random pictures are selected by the users at the time of registration. Then user has to identify the previously selected images for authentication. A set of pictures are presented on the interface to the users, some are taken from their portfolio, and some images are selected randomly. Users have to select their images, for successfulauthentication.

B. CaRP : An Overview

In CaRP, for every login attempt a new image is generated, also for the same user. CaRP scheme is clicked-based graphical password. According to memorizing and entering a password, CaRP schemes areclassified into two types: a new category and recognition.

C. Recall based techniques

Pass Points: Based on Blonder's idea [10] Pass Points is a click-based graphical password system where a password consists of a sequence of five click points on a image divided into pixels. A user must click within tolerance region for each click- point to successfully login. An improvement over Pass Points is that the users get immediate feedback about an error when trying to log in.

D. Recognition based techniques

Dhamija and Perrig [3] proposed a graphicalauthentication scheme based on the HashVisualization technique [8]. In their system, the user is asked to select a certain number of images from a set of random pictures generated by a program (figure 1).Later, the user will identify the preselected images in order to be authenticated. The average log-in time is longer than the traditional approach.

A weakness of this system is that the server needs to store the selected image set of each user in plain text. Also, the process of selecting a set of pictures from the picture databasecan be tedious and time consuming for the user. Akula and Devisetty's algorithm [9] is similar to the technique proposed by Dhamija and Perrig [3]. The difference is that by using hash function SHA-1, which produces a 20 byte output, the authentication is secure and less memory is consumed.

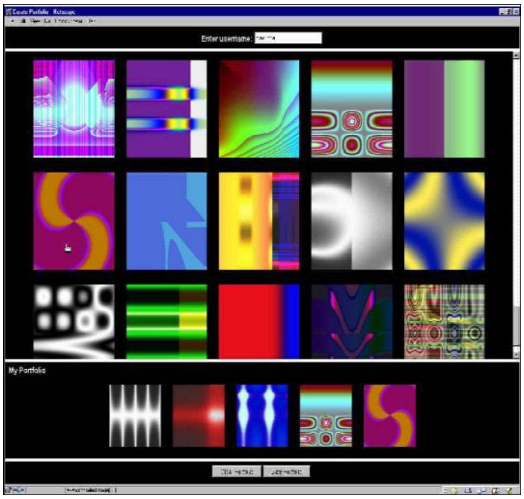

Fig. Images used by Dhamija&Perrig.

Weinshall and Kirkpatrick [6] 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. 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.

E. Combination of Recall & Recognition Based Approach

This technique is a combination of recognition and recall approach based techniques. It has two phases. First is a registration phase and second is a login phase

Registration Phase-

1. A user creates his profile by entering personal details and username.
2. Then he is presented with a set of 25 images as shown in Fig. 1. This is the common image-set for all users. The

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

user has to select any number of images from this set. Even he may choose a single image more than once. This selection will act as the password of his first step of authentication.

Fig. 1 Image-set for registration

3. Next he will choose any picture from the stored image database or from the local memory at his own choice.
4. Now he is presented with a set of questions and this image. The user has to select any three questions from the set.
5. To answer each question he will click on any point of the image. So for three questions there will be three region of-answers (ROA) within the image and each question will be associated with an ROA. Each ROA is described by a square (center and some tolerance in both X and Y axis).

Login Phase-
1. In step-1, a user is asked for his user name and graphical password (correct selection of images in a correct sequence). The order ofimages within the set will be random at every login time. This authentication step is shown in Fig. 2.

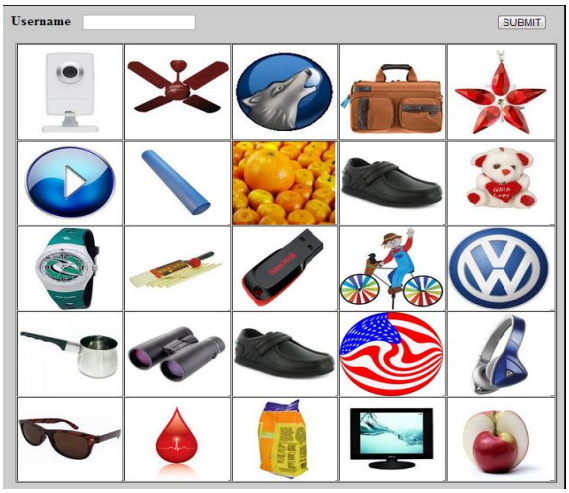

Fig. 2 Step-1 Authentication

2. After supplying this, and independent of whether or not it is correct, in step-2 authentication, the user is presented with the set of three questions and the pre-selected image.
3. The order of questions will be random. The user has to click on the correct ROAs according to the order of questions.
4. After the successful entries in both steps the user is allowed to access his account. The screenshot of the step-2 authentication is shown in Fig. 3.

IV. CONCLUSION

In this paper, we have reviewed various proposed system for Information Security using graphical passwords. We first have seen Authentication scheme involving clued click point, authentication scheme involving selection of random images from the set of images, caRP based system, pass point recall system overcoming the issues of click point systems, recognition system and combination of the both recall and recognition. The drawbacks of using recall and recognition individually are overcome by adopting combination of both recall and recognition. In our proposed system, we are using recall and recognition based system and providing two level authenticationwhich will facilitate generation of dynamic password each time user logs in.

REFERENCES

[1] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., \Murray Hill, NJ, U. S. Patent-5559961, Ed. United States, 1996.\
[2] Sonia Chiasson, P.C. Van Oorschot, and Robert Biddle, “Graphical Password Authentication Using Cued Click Points”, 12th European Symposium on Research in Computer Security (ESORICS), 2007, pp.359-374
[3] R. Dhamija, and A. Perrig. “Déjà Vu: A User Study Using Images for Authentication”. In 9th USENIX Security Symposium, 2000.
[4] Graphical Passwords: A Survey XiaoyuanSuo Ying Zhu G. Scott. Owen Department of Computer Science Georgia State University xsuo@student.gsu.edu, yzhu@cs.gsu.edu, owen@siggraph.org
[5] A New Graphical Password: Combination of Recall & Recognition Based ApproachMd. AsrafulHaque, Babbar Imam
[6] Authentication schemes for session passwords.Weinshall and Kirkpatrick
[7] 3-Level Password Authentication System. Lalu Varghese, Nadiya Mathew, Sumy Saju, Vishnu K Prasad.
[8] Hash Visualization: a New Technique to improve Real-World Security Adrian Perrig Adrian Perrig@cs.cmu.edu Dawn Song Dawn Song@cs.cmu.edu
[9] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings ojlv1idwes Instruction andComputing Symposium, 2004
[10] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.