3rd National Conference on Green Technology and Science for Sustainable Development
© 2020 IJSRST | Volume 5 | Issue 6 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
International Journal of Scientific Research in Science and Technology

Three way authentication technique using User Defined Graphical Authentication System

Miss. Payal U. Gujare[1], Dr. A. S. Kapse[2], Dr. Arvind S. Kapse[3]
*[1]M.E. Student, Computer Science and Engineering, ACE Chikhali, Maharashtra, India
[2]Head, Department of Computer Science & Engineering, Anuradha Engineering College, Sant Gadge Baba Amravati University, Chikhli, Maharashtra, India
[3]Assistant Professor, P. R. Pote College of Engineering & Technology, Amravati, India

ABSTRACT

In the field of data security, user authentication is extremely important. To enforce the security of information, passwords were introduced. User authentication is one of the important topics in information security. A strong text-based password scheme provides some degree of security. However, the very fact that strong passwords are difficult to memorize often leads their owners to write down them on papers or maybe save them during a file. A text-based password may be a popular authentication method used from the past. Text-based passwords tend to various attacks such as dictionary attacks, guessing attacks, brute force attacks and social engineering attacks, etc. An alternative solution to text-based authentication is graphical password authentication. In recent years, computer systems and Internet-based environments used graphical authentication technique for his or her user's authentication. Numerous graphical password schemes are proposed thus far because it improves password usability and security. This paper proposed the existing graphical password techniques, which are categorized into four techniques as recognition-based, pure recall-based, cued-recall based and hybrid-based.

Keywords : Graphical password, Security, Alphanumeric Password

I. INTRODUCTION

In recent years, information security has been formulated as important problem. Main area of information security is authentication which the determination of whether user should be allowed access to given system or resource. In this context, password is a common and widely authentication method. A password is a form of secret authentication that is used to control access to data. It is kept secret from unauthorized users, and those wishing to gain access are tested and are granted or denied access based on the password according to that. Passwords are used from ancient times itself as unique code to detect the malicious users. In modern times, passwords are used to limit access to protect computer operating systems, mobile phones, others etc. A computer user may need passwords for many uses such as log in to personal accounts, accessing e-mail from servers, retrieving files, databases, networks, web sites, etc. Normal passwords have drawbacks such as hacked password, forgetting password and stolen password [1]. Therefore, strong authentication is needed to secure all our applications. Conventional passwords are been used for authentication but they are known to have problems in usability and security. Recent days, another method such as graphical authentication is introduced. Graphical password are been proposed as an alternative to alphanumeric password. Psychological studies have shown that people can remember images better than text. Images are generally easier to remember than alphabets and numbers, especially photos, which are even easier to remember than random pictures.

II. EXISTING SYSTEM

Using recognition-based techniques: a user is presented with a group of images and therefore the user passes the authentication by recognizing and identifying the pictures he or she selected during the registration stage. Using recall-based techniques, a user is asked to breed something that he or she created or selected earlier during the registration stage. We proposed a graphical password mechanism for mobile devices. During the enrolment stage, a user selects a topic (e.g. sea, cat, etc.) which consists of thumbnail photos then registers a sequence of images as a password. During the authentication, the user must enter the registered images within the correct sequence. One drawback of this system is that since the amount of thumbnail images is restricted to 30, the password space is little.

III. GRAPHICAL PASSWORD METHODS

Graphical based password techniques have been proposed to solve the limitations of conventional text-based password techniques because pictures are easier to remember than texts. Graphical password techniques show that techniques can be categorized into four groups as follows.

A. Recognition-Based Technique

In this category, users select images, icons or symbols from a collection of images. At the time of authentication, the users need to recognize their images, symbols, icons which are selected at the time of registration among a set of images.

B. Recall-Based Technique

This category is very easy and convenient, but it seems that users can hardly remember their passwords. Still, it is more secure than the recognition based technique.

C. Cued Recall-Based Technique

In this category, users are provided with reminders or hints. Reminders help the users to reproduce their passwords or help users to reproduce the password more accurately. This is similar to recall based schemes but it is recalled with cueing.

D. Hybrid Schemes

In this category, the authentication will be typically the combination of two or more schemes. These schemes are used to overcome the drawbacks of a single scheme, such as spyware, shoulder surfing.

IV. PASSWORD BASED ON DRAWING SYMBOLS

In this method, a user is asked to draw any symbol like circles, triangles and etc. Which can be used to login next time. Here, the resolution or dimensions doesn’t matter. Only how the curser is moved to draw a particular pattern matters.

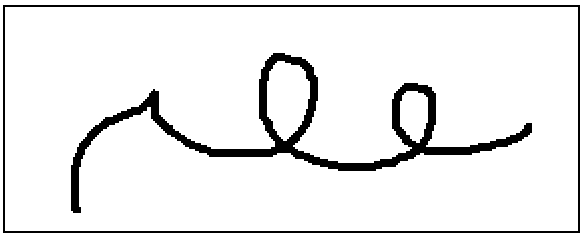


Figure 1 : Proposed Drawing Pattern

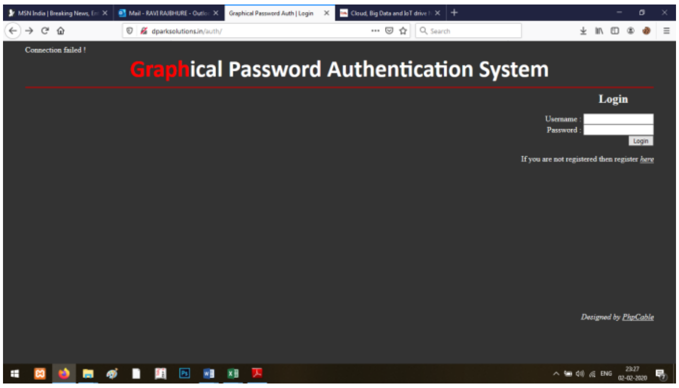
Recognition-based systems are also known as cognometric systems. These systems generally require that users must memorize the portfolio of images during the process of password creation, and when logged in, users must recognize images from decoys. The exceptional ability of humans to recognize the images previously seen made the recognition based algorithms more popular. Various recognition based systems have proposed using different types of images, mostly like faces, icons, everyday objects, random arts, etc. The user has to identify the password pictures from the challenge set of password images and decoy images. It is easy to store and transmit random art images generated by small initial seeds and also art images make it inconvenient to record or share with others. This system having drawbacks as it is hard to remember an obscure picture and corpus size is much smaller than that of text-based passwords. The cognitive authentication system computes the cumulative probability of the correct answer to ensure that was not entered by chance after each round. When the probability is above a certain threshold, authentication is a success.

V. WORKING OF SYSTEM

The process of the proposed system based on three steps as follows:

1. Simple authentication using user name and password in which user first registered itself by providing username and password and further it will authenticate using the username and password credentials.
2. The second method is using the database of the image in which n number of images can be inserted to provide higher authentication whereas previously it was limited with image quantity. The sequence of the image or the image that was selected during the registration process matched with the current selection and if matches will allow proceeding for next authentication.
3. The third authentication is based on the pattern in which we draw the image currently we are trying to draw lines circle and rectangle that system will recognize in how many numbers the combination of lines circle and rectangle was drawn and hence verifying with pattern entered previously while registration. The size of the lines circle and rectangle is now the matter in this case

VI. PROPOSED SYSTEM


MSN India | Breaking News, En
Mail - RAVI RAJBHURE - Outlo
Graphical Password Auth | Login
Cloud, Big Data and IoT drive
dparksolutions.in/auth/
Search
ENG
23:27
02-02-2020

Connection failed !

Graphical Password Authentication System

Login

Username :

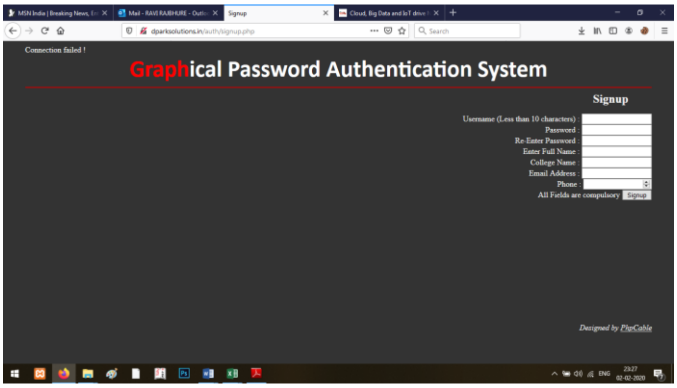
Password :

Login

If you are not registered then register here

Designed by PhpCable

Figure 2 : Authentication Page Registration


MSN India | Breaking News, En
Mail - RAVI RAJBHURE - Outlo
Signup
Cloud, Big Data and IoT drive
dparksolutions.in/auth/signup.php
Search
ENG
23:27
02-02-2020

Connection failed !

Graphical Password Authentication System

Signup

Username (Less than 10 characters) :

Password :

Re-Enter Password :

Enter Full Name :

College Name :

Email Address :

Phone :

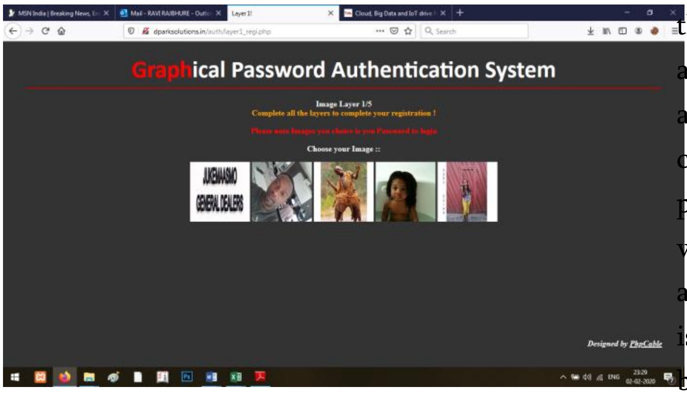
All Fields are compulsory Signup

Designed by PhpCable

Figure 3 : Registration Page

B. Using the Database of Images:

In this method, users are supposed to select images from the database in a particular sequence to login. During the creation of the password, users will be given a set of images from the database & will be asked to select the ‘n’ number of images in their own desired sequence. And next time whenever they login they will be asked to select the same set of images in that particular sequence.


MSN India | Breaking News, En
Mail - RAVI RAJBHURE - Outlo
Layer 1!
Cloud, Big Data and IoT drive
dparksolutions.in/auth/layer1_regi.php
Search
JUKEMAASMO GENERAL DEALERS
ENG
23:29
02-02-2020

Graphical Password Authentication System

Image Layer 1/5

Complete all the layers to complete your registration !

Please note Images you choice is you Password to login

Choose your Image ::

Designed by PhpCable

Figure 4 : Image Layer Level 1 of 5

VII. APPLICATION

A. Government

- Services and registrations portals
- Taxes, assessments, and other payments
- Licenses and certifications
- Document requests

B. Manufacturing

- Verifications of sensitive system access
- Vehicle driver identity
- Authenticated time clock logging
- Protect access to intellectual property

C. Professional Associations

- High-value exams and credentialing
- Compliance and certifications

VIII. VIII. CONCLUSION AND FUTURE ASPECTS

A novel Graphical Password scheme is proposed during this paper which tries to satisfy the standards of simple use and therefore the security at an equivalent time. The scheme has a large password space and the simple implementation makes it easy for the user to create a password and memorize it too. The main reason for using a graphical password is they are more secure and can be recalled easily. Graphical password techniques achieve better security than conventional textual passwords. They are more accurate and reliable than textual passwords. Different algorithms from recognition-based, pure recall based, cued recall-based, and hybrid schemes of graphical password authentication are reviewed. In this paper, we identify several advantages of graphical password authentication. Therefore, it can be concluded that it is more difficult to break graphical passwords than to break alphanumeric passwords.

IX. REFERENCES

[1]. International Conference On Emanations in Modern Technology and Engineering (ICEMTE-2017) ISSN: 2321-8169 Volume: 5 Issue: 3 56 – 58

[2]. Eluard, M.; Maetz, Y.; Alessio, D., “Action-based graphical password: Click-a-Secret”, 2011 IEEE International Conference on Consumer Electronics, 2011, pp.265-266.

[3]. P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, “Purely automated attacks on pass points-style graphical passwords,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 393–405, Sep. 2010.

[4]. Umar, M.S.; Rafiq M.Q. Ansari J.A.,”Graphical user authentication: A time interval based approach"; Signal Processing Computing and Control (ISPCC), 2012 IEEE International Conferencettsburgh, Pennsylvania, USA, ACM

[5]. X. Suo, Y. Zhu, and G. S. Owen, "Graphical Passwords: A Survey", in Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005), IEEE Computer Society, pp. 463-472, 2005.

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