IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 3, Issue 6)
Available online at www.ijariit.com

Graphical Authentication for Web Based Application

Aditya Badhe
AISSMS College of Engineering, Pune
addibadhe18@gmail.com

Dhananjay Dahake
AISSMS College of Engineering, Pune
dhananjaydhk1@gmail.com

Prajakta Rokade
AISSMS College of Engineering, Pune
prajaktarokade28@gmail.com

Arati Dhakane
AISSMS College of Engineering, Pune
aratidhakane@gmail.com

D. M. Ujlambkar
AISSMS College of Engineering, Pune
dmujlambkar@aissmscoe.com

Abstract: User authentication is an important topic in the field of information security. To enforce security of information, passwords were introduced. Text based password is a popular authentication method used from ancient times. However text based passwords are prone to various attacks. Strong text-based password schemes could provide with certain degree of security. However, the fact that strong passwords are difficult to memorize often leads their users to write them down on papers or even save them in a computer file. Human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as the weakest link in the authentication chain. Graphical password is one of the alternative solution to alphanumeric password as it is very simple process to remember alphanumeric password. One of the major reasons behind this method implementation is that, according to psychological studies human mind can easily remember images than alphabets or digits. Graphical authentication has been proposed as a possible alternative solution to text-based authentication. A new technique of captcha and OTP is being used for the verification purpose. Three times a person is given chance to try for login if the person fails then he is blocked till the session expires.

Keywords: Graphical Password, OTP, Security, User Authentication, Web Application.

I. INTRODUCTION

Initially all the web authentication was done on the basis of text password. Text password was the only system used for authentication system. But as time goes on this system finds many disadvantages to use it. As like this was not trusted as it had always threat of getting hacked. Text password always tested the memory of the user, so it wasn't good system. The basic concept of this system is simply the interaction of user with sequence of images. The basic goal of this system is to achieve higher security with simple technique to use by a user and harder to guess by a hacker. Image password authentication system is best alternative for text password. This system provides user-friendly environment for the users with a kind of image interaction. Here the password need not be a string of characters it can use few images this may be easy for the users to remember. Then the graphical password authentication system creates the great impact on authentication system, initially pass point and persuasive click point were the systems used as the alternative of the text password. A new technique of image password and OTP is being used for the verification purpose. 3 times a person is given chance to try for login if the person fails then he is blocked till the session expires. Image Password is a computer program or system intended to distinguish human from machine input, typically as a way of thwarting spam and automated extraction of data from websites. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to something a person has (such as a specific cellphone).Then the Image Password input is been inserted and login is decided whether it is authenticated or not.

A user in this system is associated with a few trustees that were selected from the user's friends. When the user wants to regain access to the account, the service provider sends different verification codes to the user's trustees.

II. PROBLEM DEFINITION

Security practitioners and researchers have made studies in protecting systems, individual users and digital assets. The password problem arises largely from limitations of human's long-term memory (LTM). Once a password has been chosen and learned the user must be able to recall it to log in. But, people regularly forget their passwords. Graphical passwords introduce us to a whole new form of authentication. The most common form of authentication used today is the used of alphanumeric texts and this form of authentication has been proven to be prone to several forms of attacks. Since it is easier to remember pictures than text, graphical passwords tend to enhance security and at the same time make it easier for the user to use and access data.

III. LITERATURE SURVEY

[1] A Survey on Different Graphical Password Authentication Techniques.

Author: Saranya Ramanan, Bindhu J S

Description

A comprehensive survey of the existing graphical password techniques is conducted. These techniques are categorized into four types: recognition-based, pure recall-based, cued-recall based and hybrid approaches. Here the strengths and drawbacks of each method are analysed. This survey will be particularly useful for researchers who are interested in developing new graphical password algorithms as well as industry practitioners who are interested in deploying graphical password techniques.

[2] Enhancement of Password Authentication System Using Graphical Images.

Author: Amol Bhand, Vaibhav desale, Swati Shirke, Suvarna Pansambal (Shirke)

Description

The Enhancement of password authentication system with the help of images is proposed. This paper mainly focuses on the concept of graphical password system. It is supported by the using cued click points for authentication purpose. The basic concept of this system is simply the interaction of user with sequence of 5 images. The basic goal of this system is to achieve higher security with simple technique to use by a user and harder to guess by a hacker. Graphical password authentication system is best alternative for text password. Cued click point (CCP) is best alternative to old graphical password system. CCP is combination of five click points on particular five images. In this this paper, CCP is clubbed with new technologies like mobile phones and E-mail.

[3] A Shoulder Surfing Resistant Graphical Authentication System.

Author: Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng

Description

A novel authentication system called Pass Matrix, based on graphical passwords to resist shoulder surfing attacks is proposed. With a one-time valid login indicator and circulate horizontal and vertical bars covering the entire scope of pass-images, Pass Matrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera based attacks. Implementation of a Pass Matrix prototype on Android was done and carried out real user experiments to evaluate its memorability and usability. From the experimental result, the proposed system achieves better resistance to shoulder surfing attacks while maintaining usability.

[4] Graphical Authentication System Using Pass Matrix.

Author: Sarojini, Priya, Bhuvaneshwari

Description

Authentication based password is largely used in the computer security and privacy. Most of the traditional passwords are numbers and alphabets character. That can be easily identified by the unauthorized people. The identification leads the shoulder surfing attacks. However, human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as the weakest link in the authentication chain. With web applications and mobile apps piling up, people can access these applications anytime and anywhere with various devices. To overcome these problems a novel authentication system called Pass Matrix resist shoulder surfing attacks was proposed.

[5] Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice.

Author: Susan Wiedenbeck, JimWater, Jean-Camille Birget, Alex Brod-skiy, Nasir Memon

Description

The human factors testing was expanded by studying two issues: the effect of tolerance, or margin of error, in clicking on the password points and the effect of the image used in the password system. The results show that accurate memory for the password is strongly reduced when using a small tolerance (10x10 pixels) around the user's password points. This may occur because users fail to encode the password points in memory in the precise manner that is necessary to remember the password over a lapse of time.

In this image study compared user performance on four everyday images. The results indicate that there were few significant differences in performance of the images. This preliminary result suggests that many images may support memorability in graphical password systems.

[6] On the Security of Trustee-Based Social Authentications.
Author: Neil Zhenqiang Gong, Student Member, IEEE and DiWang

Description

A systematic study about the security of trustee based social authentications is done. In particular, first a novel framework of attacks was introduced, which is called forest fire attacks. In these attacks, an attacker initially obtains a small number of compromised users, and then the attacker iteratively attacks the rest of users by exploiting trustee-based social authentications. Then a probabilistic model is constructed to formalize the threats of forest fire attacks and their costs for attackers. Moreover, we introduce various defence strategies. Finally, framework is applied to extensively evaluate various concrete attack and defence strategies using three real-world social network datasets. Results have strong implications for the design of more secure trustee-based social authentications.

[7] When the Password Doesn't Work: Secondary Authentication for Websites.
Author: Robert Reeder, Stuart Schechter

Description

Nearly all websites that maintain user-specific accounts employ passwords to verify that a user attempting to access an account is, in fact, the account holder. However, websites must still be able to identify users who can't provide their correct password, as passwords might be lost, forgotten, or stolen. In this case, users will require a form of secondary authentication to prove that they are who they say they are and regain account access. Websites can use a variety of secondary authentication. The article discusses secondary authentication mechanisms, emphasizing the importance of assembling an arsenal of mechanisms that meet user's security and reliability needs.

IV. PROPOSED SYSTEM

Secure graphical authentication system is offered that protects users from becoming fatalities of attacks when inputting passwords in public through the usage of click points on the image password. In this scheme, the next image is displayed based on the basis of the correct location of the previous click-point. After correctly clicking on the password the user will be authenticated or vice versa. The wrong input for 3 times will lead to blocking the user. The user can be unblocked by the admin or user has to go through 3 layer security consisting of OTP, Security Question and Image password. This system is more easy to use and user friendly. This provides better security against brute force attacks, dictionary attack since users use a dynamic click point to point out the position of their password. It has a wide range of use on web based applications.

V. SYSTEM ARCHITECTURE

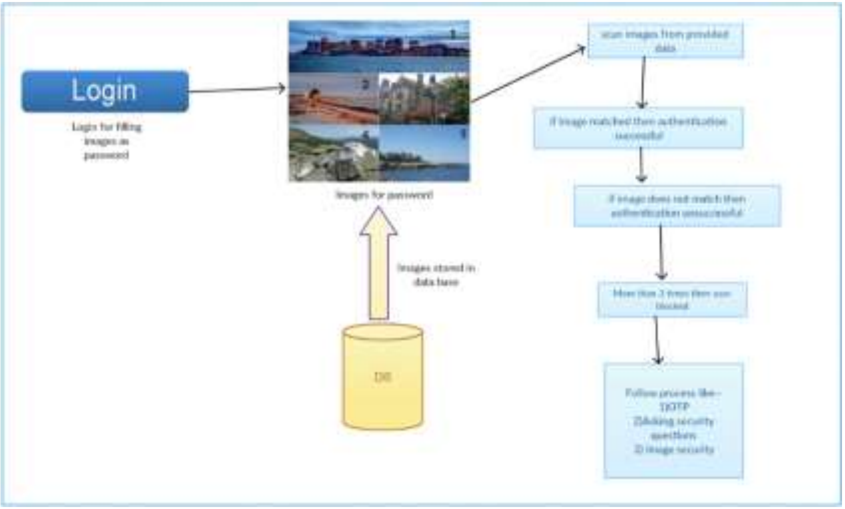
Login
Login for filling images as password
1
2
3
4
5
Images for password
Images stored in data base
DB
scan images from provided data
If image matched then authentication successful
If image does not match then authentication unsuccessful
More than 3 times then user blocked
Follow process like–
1)OTP
2)Asking security question
3) image security

Fig.1: System Architecture

First of all the system registers the respective user into the system, then it starts and ask the user for credentials to access the system. Then the system proceeds through the credentials verification and the system tasks as shown in the Figure that is the online tasks of system begins by accessing the resources and authenticate the respective user according to his credential used at the registration phase. Then after collection of this data it is stored in a database.

After this some pre-processing and verification of this data is done and user get the access to data. The registration phase of the user is done on the primary basis and it is in the form of three layer security as registration through image password, security question and OTP. This data is stored in the database in the background and the server will operate its functionality. Then the user has to login to his account through image password and then the algorithm will work and data will get verified and if it turns correct he is given access to his data. Then all this procedure is done and user access his data from the web application.

VI. CONCLUSION

Graphical Password schemes provide a way of making more human friendly passwords. Here security of system is quite high. Dictionary attacks and brute force search are also infeasible. On studying the human phycology we can conclude that graphical password are more easily remembered than text passwords. Graphical password authentication system can be used in various banking, shopping websites, email system etc. Graphical password authentication system can be time consuming, can need more storage space than text password and be prone to shoulder surfing attacks.

REFRENCES

1. Saranya Ramanan, Bindhu J S,*" A Survey on Different Graphical Password Authentication Technique*", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 12, December 2014.
2. Amol Bhand, Vaibhav desale, Swati Shirke, Suvarna Pansambal (Shirke), *"Enhancement of Password Authentication System Using Graphical Images"*. 2015 International Conference on Information Processing (ICIP) Vishwakarma Institute of Technology. Dec 16-19, 2015.
3. Hung-Min Sun,Shiuan-Tung Chen,Jyh-Haw Yeh and Chia-Yun Cheng, *"A Shoulder Surfing Resistant Graphical Authentication System"*.DOI10.1109/TDSC.2016.2539942, IEEE.
4. Sarojini, Priya, Bhuvaneshwari, *"Graphical Authentication System Using Pass Matrix"*.International Journal of Computer Trends and Technology(IJCTT) Special Issue April – 2017.
5. Susan Wiedenbeck, Jim Water, Jean-Camille Birget, Alex Brod-skiy, Nasir Memon, *"Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice"*.
6. Neil Zhenqiang Gong, Student Member, IEEE and DiWang.*"On the Security of Trustee-Based Social Authentications"*. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 8, AUGUST 2014.
7. Robert Reeder, Stuart Schechter, *"When the Password Doesn't Work: Secondary Authentication for Websites"*. IEEE Security & Privacy (Volume: 9, Issue: 2, March-April 2011).