Journal of Advanced Research in Technology and Management Sciences
Volume: 04 Issue: 02 ISSN: 2582-3078 April-May 2022
Available online at: http://www.jartms.org

GRAPHICAL PASSWORD AUTHENTICATION

Mr.G. MANTHRU NAIK M.Tech(PhD),Associate Professor,Dept of CSE, KHIT, Guntur
P.PRASANNA, Kallam Haranadhareddy Institute of Technology,Guntur
V.VENKATA SAI TEJA, Kallam Haranadhareddy Institute of Technology,Guntur
P. BHANUPRAKASH, Kallam Haranadhareddy Institute of Technology,Guntur
P.PRABHAKAR, Kallam Haranadhareddy Institute of Technology,Guntur

ABSTRACT

Authentication dependent on passwords is utilized generally in applications for security and protection. Still, human actions, as an example, choosing bad passwords and contributing passwords in square measures are viewed as "the most fragile connection" in the Authentication chain. Maybe than discretionary alphanumeric strings, clients will pick passwords either short or significant for simple memorization. With web applications and versatile applications accumulation, individuals can get to these applications whenever and anyplace with various gadgets. This advancement brings extraordinary accommodation yet, in addition, builds the likelihood of presenting passwords to bear riding attacks. Attackers can notice straightforwardly or utilize outside recording gadgets to gather client's qualifications. To avoid this sort of issue, we need another method of confirmation. Here, we can choose a graphical authentication method. The image password offers the best approach to sign on that is simpler than recollecting and composing along with simple passwords. You can sign in by tapping the right points or creating the right gestures over an image that you just select in advance. either short or from the word reference, instead of irregular alphanumeric strings. Human actions such as selecting bad passwords for new accounts and inputting wrong passwords in an insecure way for later logins are regarded as the weakest link in the chain of authentication. Shoulder surfing occurs when someone watches over your shoulder to collect valuable or personal information such as your password, ATM PIN, or credit card number, as you key it into an electronic device.

INTRODUCTION

User Authentication is an interaction that permits a gadget to approve the character of an individual who associates with network assets. Commonly textual passwords are the most used form of authentication for all websites and applications. Textual passwords consist of a string of characters which may also include special characters and numbers. In most cases, users may use only one username and password for multiple accounts. But they are not fully secured. So, we should maintain strong passwords, comprising numbers, uppercase, and lowercase letters. Then these textual passwords are considered strong enough to resist brute force attacks. However, a strong textual password is hard to remember and recall. Along these lines clients will in general pick passwords that are either short or from the word reference, instead of irregular alphanumeric strings. Human actions such as selecting bad passwords for new accounts and inputting wrong passwords in an insecure way for later logins are regarded as the weakest link in the chain of authentication. Shoulder surfing occurs when someone watches over your shoulder to collect valuable or personal information such as your password, ATM PIN, or credit card number, as you key it into an electronic device. A strong textual password is hard to memorize and recollects.

LITERATURE SURVEY

Wantong Zheng and Chun fu Jia proposed a method “Combined PWD”. This scheme proposes an online secret phrase verification component, combined PWD, through embedding separators (e.g., spaces) into the passwords to reinforce the current secret word validation framework. This plan uses the custom of the client’s input. In this examination site clients can embed spaces in their secret word where they need to stop when they register a record, and the site back-end records the number of spaces in each hole In the paper

A novel time-based unique password was contributed to avoiding challenges focusing a third party such as one- time password email, test and token

device, the client will set an underlying secret word to characterize how the secret key will be changing throughout a characterized time, we tracked down that the framework. Then found that the system retains the strength of the dynamic password and improves the usability of the system in terms of availability A strong password authentication scheme was proposed by Yang Jing boo. The one-time password authentication schemes can be divided into two types namely weak password authentication schemes and strong-password authentication schemes.

In this paper, we survey the as of W.C Ks scheme and it also shows an attack against his protocol. And also found that strong passwords have higher strength and easily guessing is not possible. Later, we present a strong password authentication scheme. This paper expands W. C. Ku's plan so that the alteration convention can oppose Stolen-verifier assault. The changed convention is built without loss of effectiveness

Hua Wang, Yao Guo proposes another reuse- situated secret phase authentication system, called Desktop Password Authentication Center (DPAC), to reuse counter-measures among applications, along these lines lessening the expense of protecting passwords against dangers. This arrangement can take out a ton of tedious work and reduces the expense essentially, we demonstrate the feasibility of DPAC by implementing a prototype, in which we migrate the widely used OpenSSH to DPAC and implement two example countermeasures

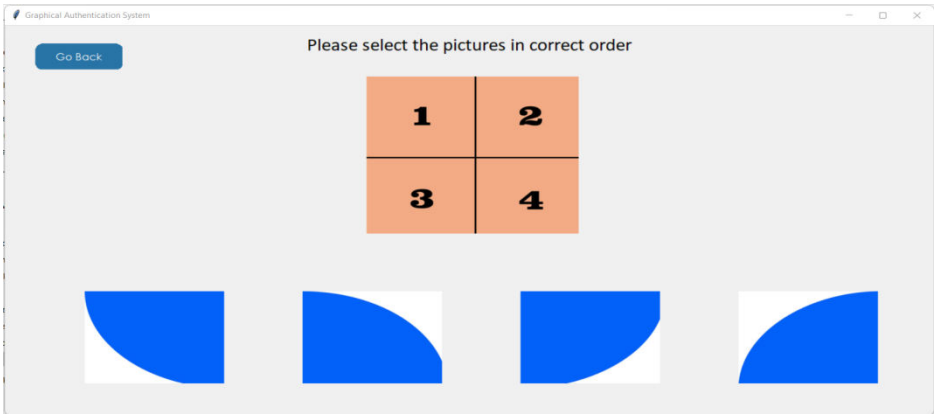
Password authentication code (PAC) is a very important issue in many applications such as web- sites and database systems etc. Salah Refish proposes a PAC-RMPN scheme. In this paper, PAC between two clients to affirm verification between them has been introduced. This research presents a novel solution to the era-long problem of password authentication at the incoming level. They should discover a strategy to secure this a secret word from anticipated attackers. A legitimate user types his password only and presses enter to propagate it to another user which he wants to be authenticated

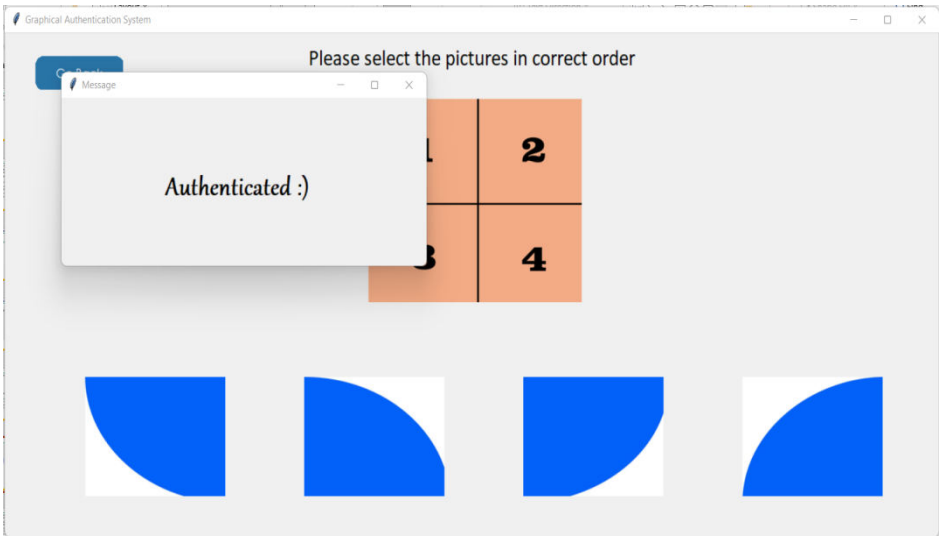
Journal of Advanced Research in Technology and Management Sciences
Volume: 04 Issue: 02 ISSN: 2582-3078 April-May 2022
Available online at: http://www.jartms.org

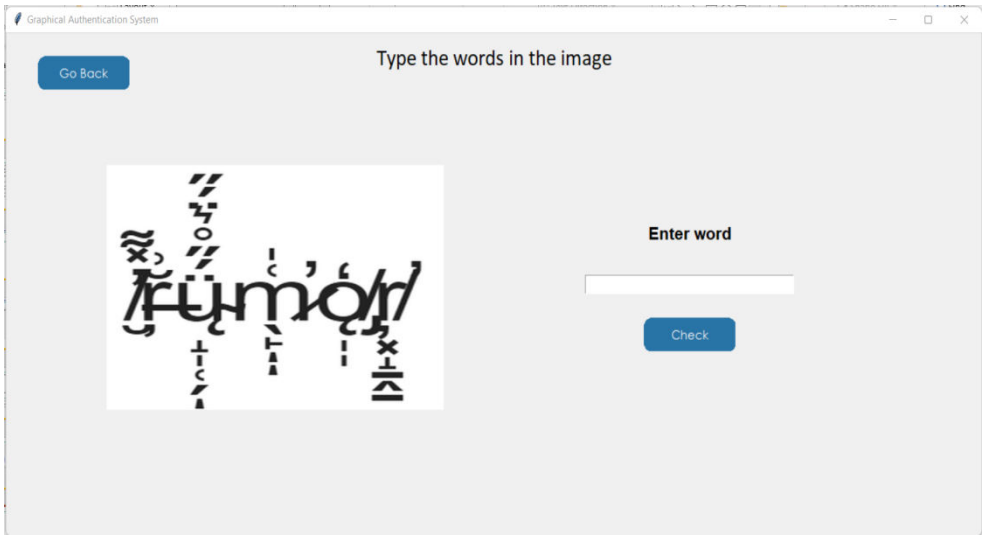
PROPOSED

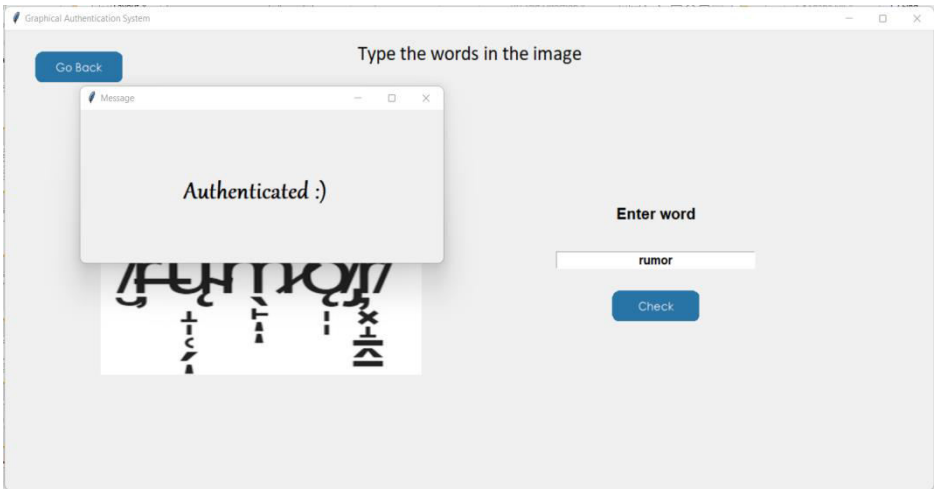
The proposed system is graphical password based. According to a study, the human brain has a greater capability of remembering what they see(pictures) rather than alphanumeric characters. Therefore, graphical passwords overcome the disadvantage of alphanumeric passwords.The system support the following 2 types of authentication methods: Recognition based Authentication: A user is given a set of images and he has to identify the image he selected during registration. Garbled Image Authentication: A user will be displayed a Garbled text whose readability will be really low, and user will be asked to read and then type in the text.

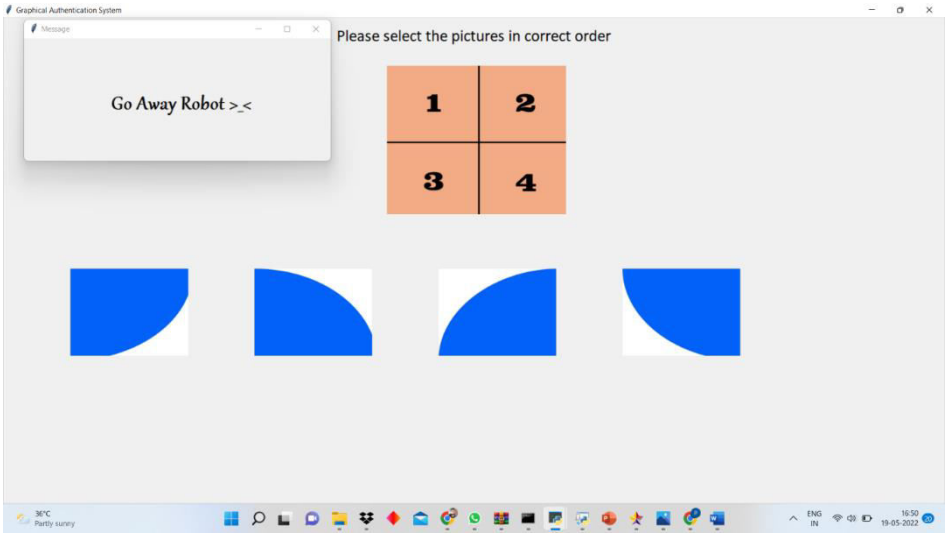
RESULTS






Graphical Authentication System
Type the words in the image
Go Back
Enter word
Check


Graphical Authentication System
Type the words in the image
Go Back
Message
Authenticated :)
Enter word
rumor
Check


Graphical Authentication System
Message
Go Away Robot >_<
Please select the pictures in correct order
1
2
3
4

CONCLUSION

User authentication is a fundamental component in most computer security contexts. In this extended abstract, we proposed a simple graphical password authentication system Although the main use for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, which provides high security compared to previous existing system.

REFERENCES

[1] Wantong zheng, Chunfu Jia,'Combined PWD: A New Password Authentication Mechanism Using Separators Between Keystrokes": 2017 13th International Conference on Computational Intelligence and Security (CIS)

[2] Salisu Ibrahim Yusuf, Moussa Mahamat Boukar, 'User Define Time Based Change Pattern Dynamic Password Authentication Scheme', 2018 14th International Conference on Electronics Computer

[3] Yang Jingbo, Shen Pingping,' A secure strong password authentication protocol", 2010 2nd International Conference on Software Technology and Engineering

[4] Hua Wang, Yao Guo, Xiangqun Chen,' DPAC: A Reuse-Oriented Password Authentication Framework for Improving Password Security", 2008 11th IEEE High Assurance Systems Engineering Symposium