

Web Based Graphical Password Authentication System

Shaik Mehboob Basha¹, K.Kumara Swamy²

¹MCA Student, Dr.K.V.Subba Reddy Institute of Technology, Kurnool, Andhra Pradesh, India

²Assistant Professor, Dr.K.V.Subba Reddy Institute of Technology, Kurnool, Andhra Pradesh, India

Abstract

Graphical passwords provide a promising alternative to traditional alphanumeric passwords. They are attractive since people usually remember pictures better than words. In this extended abstract, we propose a simple graphical password authentication system. We describe its operation with some examples, and highlight important aspects of the system.

Keywords: Password, web, authentication

Introduction

User authentication is a fundamental component in most computer security contexts. It provides the basis for access control and user accountability [1]. While there are various types of user authentication systems, alphanumeric username/passwords are the most common type of user authentication. They are versatile and easy to implement and use.

Alphanumeric passwords are required to satisfy two contradictory requirements. They have to be easily remembered by a user, while they have to be hard to guess by impostor [2]. Users are known to choose easily guessable and/or short text passwords, which are an easy target of dictionary and brute-forced attacks [3, 4, 5]. Enforcing a strong password policy sometimes leads to an opposite effect, as a user may resort to write his or her difficult-to-remember passwords on sticky notes exposing them to direct theft.

In the literature, several techniques have been proposed to reduce the limitations of alphanumeric password. One proposed solution is to use an easy to remember long phrases (passphrase) rather than a single word [6]. Another proposed solution is to use graphical passwords, in which graphics (images) are used instead of alphanumeric passwords [7]. This can be achieved by asking the user to select regions from an image rather than typing characters as in alphanumeric password approaches.

In this extended abstract, we propose a graphical password authentication system. The system combines graphical and text-based passwords trying to achieve the best of both worlds. In section 2, we provide a brief review of graphical passwords. Then, the proposed system is described in section 3. In section 4, we briefly discuss implementation and highlight some aspects about the proposed system.

Existing System

Graphical passwords refer to using pictures (also drawings) as passwords. In theory, graphical passwords are easier to remember, since humans remember pictures better than words [8]. Also, they should be more resistant to brute-force attacks, since the search space is practically infinite.

In general, graphical passwords techniques are classified into two main categories: recognition-based and recall-based graphical techniques [7]. In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images he or she chooses during the registration stage. In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

Passfaces is a recognition-based technique, where a user is authenticated by challenging him/her into recognizing human faces [9]. An early recall-based graphical password approach was

introduced by Greg Blonder in 1996 [10]. In this approach, a user create a password by clicking on several locations on an image. During authentication, the user must click on those locations. PassPoints builds on Blonders idea, and overcomes some of the limitations of his scheme [2]. Several other approaches have been surveyed in the following paper [7].

Proposed System

The proposed authentication system works as follows. At the time of registration, a user creates a graphical password by first entering a picture he or she chooses. The user then chooses several point-of-interest (POI) regions in the picture. Each POI is described by a circle (center and radius). For every POI, the user types a word or phrase that would be associated with that POI. If the user does not type any text after selecting a POI, then that POI is associated with an empty string. The user can choose either to enforce the order of selecting POIs (stronger password), or to make the order insignificant.

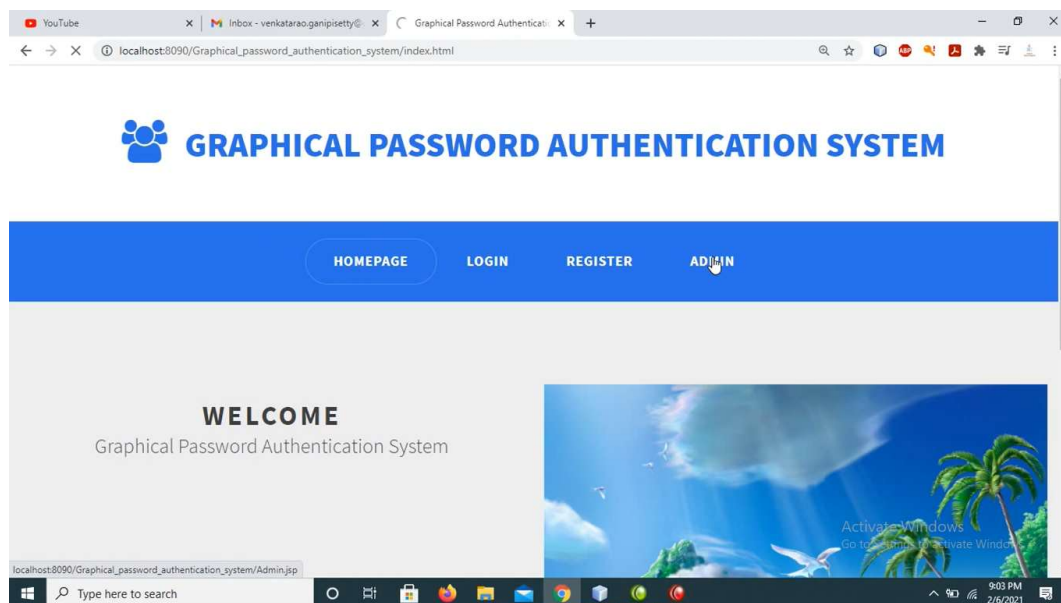
Results

Graphical password system offers a strong security against brute force and guessing attacks as it has two level of graphical passwords system. The password system is difficult to guess the password system by a person and it is a shoulder-surfing resistance system. It has a very large password range. For this project we used 3 level of security authentication following

For step1: Authentication of text base password.

For step2: Colour Base Authentication.

For step3: Image Base Authentication





YouTube | Inbox - venkatarao.ganipisetty@ | Graphical Password Authentica... | +

localhost:8090/Graphical_password_authentication_system/AdminHome.jsp?msg=success

GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

HOME PAGE VIEW PROFILE LOGOUT

WELCOME ADMIN HOME

localHost:8090/Graphical_password_authentication_system/AdminHome.jsp?msg=...

Type here to search

Graphical password authentication system - NetBeans IDE 8.1

File Edit View Navigate Source Refactor Run Debug Profile Team Tools Window Help

Search (Ctrl+F)

Projects | Files | Services

- Adaptive Diffusion of Sensitive Information In Online Social Networks
- Attendance Management System
- Authentication and Key Agreement Based on Anonymous
- A Verifiable Semantic Searching Scheme by Optimal Matching
- Car Rental System
- College Information Management System
- E-HealthCare Management System
- Graphical password authentication system
 - Web Pages
 - Source Packages
 - com.dbcon
 - DBCon.java
 - Queries.java
 - com.image
 - Libraries
 - Configuration Files
 - HROperationManager
 - Leight weight privacy preserving msg authentication
 - Mid-Day Meal Analytics
 - mlitry_rental_system
 - Online Food Ordering System
 - Online Quiz
 - Online Shopping For Gadgets
 - Online User Behavior analysis on graphical model
 - OnlineVenueBooking
 - Pay as You Decrypt Decryption Outsourcing
 - Privacy-preserving Medical Treatment System
 - Protecting user data in profile-matching social networks
 - SECURE INTRUSION RECOGNITION NETWORK FOR AN IRREGULAR COVER
 - Student Counselling Management System

index.html | aDViewProfile.jsp

```
1 /*
2  * To change this license header, choose License Headers in Project Properties.
3  * To change this template file, choose the template file in the source file folder.
4  * and open the template file in the editor.
5  */
6 package com.dbcon;
7 import java.sql.*;
8 /**
9  *
10  * @author Acer
11  */
12 public class DBCon {
13     public static Connection conn;
14     public static Connection getConn() {
15         try {
16             Class.forName("com.mysql.jdbc.Driver");
17             conn=DriverManager.getConnection("jdbc:mysql://localhost:3306/shuffle","root","");
18         } catch (Exception e) {
19             System.out.println(e);
20         }
21     }
22 }
```

Camtasia Recorder - Record...

Record | Pause | Stop | Delete | Effects | Options

Output | HTTP Server Monitor

Graphical_password_authentication_system (run) x Apache Tomcat 8.0.27.0 Log x Apache Tomcat 8.0.27.0

06-Feb-2021 21:04:37.422 INFO [http-nio-8090-exec-5] org.apache.jasper.servlet.Tid 06-Feb-2021 21:04:37.430 INFO [http-nio-8090-exec-5] org.apache.catalina.core.Stan com.mysql.jdbc.exceptions.jdbc4.MySQLSyntaxErrorException: Unknown database 'shuff java.lang.NullPointerException com.mysql.jdbc.exceptions.jdbc4.MySQLSyntaxErrorException: Unknown database 'shuff java.lang.NullPointerException


Type here to search

9:03 PM 2/6/2021



YouTube | Inbox - venkatarao.ganipisetty | Graphical Password Authenticati... | +

localhost:8090/Graphical_password_authentication_system/login.jsp



GRAPHICAL PASSWORD AUTHENTICATION SYSTEM


[HOMEPAGE](#) [LOGIN](#) [REGISTER](#)

WELCOME LOGIN HERE

UserName

Password


[Don't Have an Account ? Register](#)



Activate Windows
Go to Settings to activate Windows.

YouTube | Inbox - venkatarao.ganipisetty | Graphical Password Authenticati... | +

localhost:8090/Graphical_password_authentication_system/register.jsp



GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

[HOMEPAGE](#) [LOGIN](#) [REGISTER](#)

WELCOME LOGIN HERE


ID

Name

Email

Mobile

address



Activate Windows
Go to Settings to activate Windows.




YouTube | Inbox - venkatarao.ganipisetty | Graphical Password Authentici... | +

localhost:8090/Graphical_password_authentication_system/register.jsp

WELCOME LOGIN HERE

ID
Name
Email
Mobile
address
UserName
Password
Image1 No file chosen

[Already Have an Account ?Login](#)



Activate Windows
Go to Settings to activate Windows.

Type here to search

YouTube | Inbox - venkatarao.ganipisetty | Graphical Password Authentici... | +

localhost:8090/Graphical_password_authentication_system/Upload.jsp?msg=success


GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

HOMEPAGE LOGIN REGISTER

WELCOME UPLOAD MORE

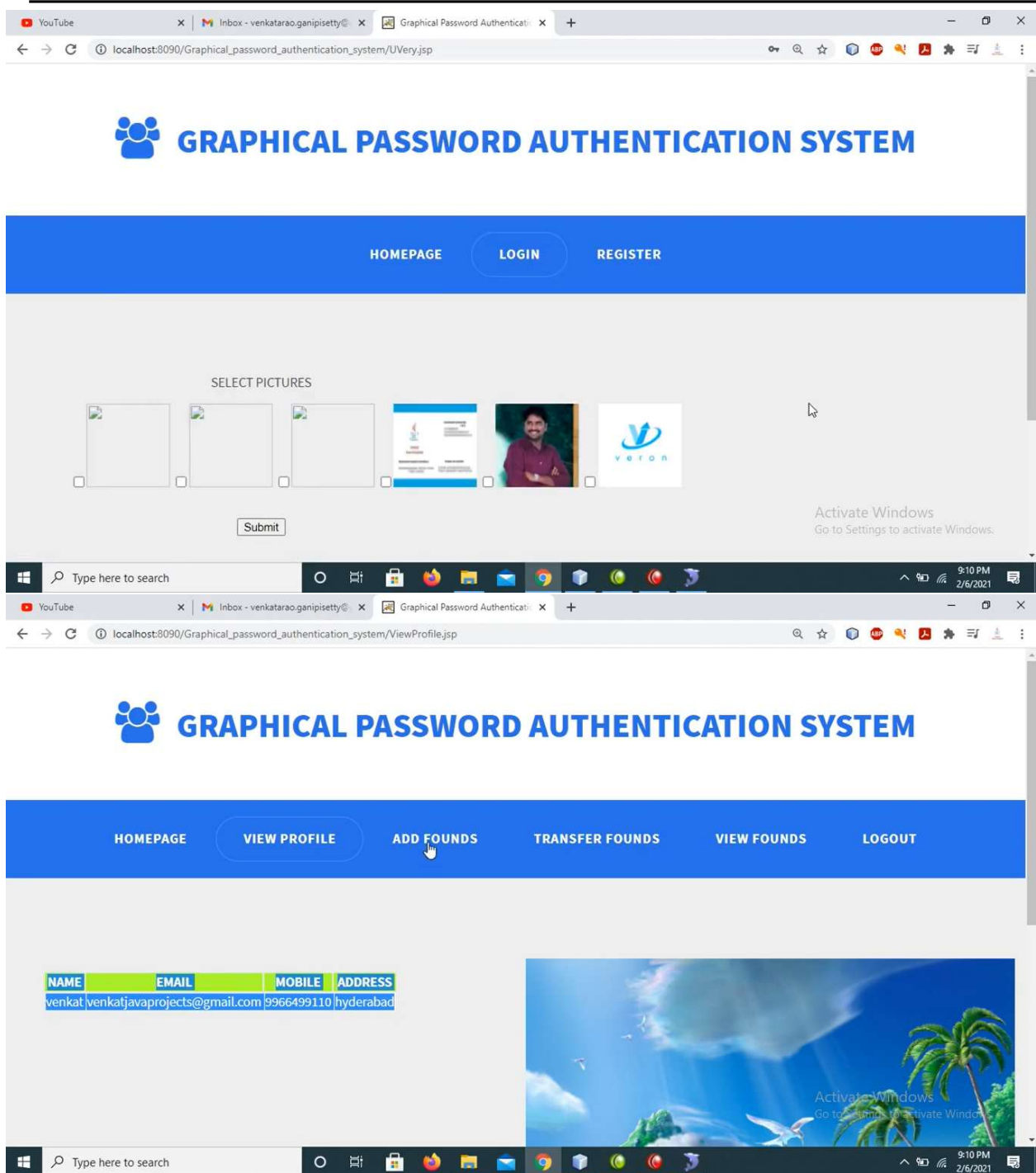
ID
Image2 No file chosen

[Already Have an Account ?Login](#)



Activate Windows
Go to Settings to activate Windows.

Type here to search



Conclusion

User authentication is a fundamental component in most computer security contexts. In this extended abstract, we proposed a simple graphical password authentication system. The system combines graphical and text-based passwords trying to achieve the best of both worlds. It also provides multi-factor authentication in a friendly intuitive system. We described the system operation with some examples, and highlighted important aspects of the system.



References

- [1] William Stallings and Lawrie Brown. Computer Security: Principle and Practices. Pearson Education, 2008.
- [2] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. Passpoints: design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, 63:102–127, July 2005.
- [3] Robert Morris and Ken Thompson. Password security: a case history. *Communications of the ACM*, 22:594– 597, November 1979.
- [4] Daniel V. Klein. Foiling the Cracker: A Survey of, and Improvements to, Password Security. In *Proceedings of the 2nd USENIX UNIX Security Workshop*, 1990.
- [5] Eugene H. Spafford. Observing reusable password choices. In *Proceedings of the 3rd Security Symposium*. Usenix, pages 299–312, 1992.
- [6] Sigmund N. Porter. A password extension for improved human factors. *Computers & Security*, 1(1):54 – 56, 1982.
- [7] Xiaoyuan Suo, Ying Zhu, and G. Scott Owen. Graphical passwords: A survey. In *Proceedings of Annual Computer Security Applications Conference*, pages 463–472, 2005.
- [8] Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud. Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies*, 63:128–152, July 2005.
- [9] Real User Corporation. The science behind passfaces, June 2004.
- [10] G. E. Blonder. Graphical password. U.S. Patent 5559961, Lucent Technologies, Inc. (Murray Hill, NJ), August 1995.