

Text-based Graphical Password System to Enhance Security

Athira S.^{1,*}, G. Rajiv Suresh Kumar², M. Rupa³

Abstract

A graphical password is a type of authentication that requires the user to choose from a set of images in a certain order. For most people, remembering a graphical password is easier than remembering a text-based password. Passwords with graphics may be more difficult to remember. offer better security than text-based passwords. Humans can remember pictures much better than the text. To create passwords more memorable and less vulnerable to security attacks. A text-based movable frame graphical password system is proposed. The system includes both the Graphical and Text- based images interface for identification. It displays a grid which is either graphical images, or alphabets or multiple/mixed alphabets. Traditional text- based password schemes are subjected to dictionary attacks. Graphic password systems, which use graphics instead of words as a password, are a promising alternative to text-based recognition schemes. These are again affected due to shoulder surfing and less effective due to large dictionary space. providing a solution based on text-based graphical password techniques. Our research has a main objective: To enhance the security. The graphical password system with multiple alphabet images is more recognizable. It has less cognitive load on user as compared to image based graphical password schemes.

Keywords: Authorization security, secured logging, intruders, hackers, unauthorized user

INTRODUCTION

Password systems are usually simple text-based; graphical image based which are more vulnerable to different kinds of attacks. Password systems should less predictable and strong passwords with more memorability and security. Traditional password systems vulnerable attacks, including shoulder surfing, dictionary attacks, man in the middle attack and eavesdropping etc. The passwords might be easily guessed by the attacker. If a password is hard to guess by an attacker or outsider, then it is also

hard to remember by the user. One can remember pictures easily than a text. This fact has been proposed graphical password schemes as a feasible method to text-based schemes. Which may also have disadvantages over some attacks. Here we propose a system with graphical password scheme which we choose a random image as a password and, we can upload an image as a permanent password which would be easy to remember to the user [1–5].

*Author for Correspondence

Athira S.

¹Assistant Professor, Department of Computer Science Engineering, JCT College of Engineering and Technology, Coimbatore, Tamil Nadu, India

²Professor, Department of Computer Science Engineering, JCT College of Engineering and Technology, Coimbatore, Tamil Nadu, India

³Assistant Professor, Department of Computer Science Engineering, JCT College of Engineering and Technology, Coimbatore, Tamil Nadu, India

Received Date: November 23, 2021

Accepted Date: December 21, 2021

Published Date: December 29, 2021

Citation: Athira S., G. Rajiv Suresh Kumar, M. Rupa. Text-based Graphical Password System to Enhance Security. Trends in Opto-electro & Optical Communication. 2021; 11(3): 8–14p.

EXISTING SYSTEM

The existing password security system include text-based, 8-digit codes, pattern lock, fingerprint lock, face recognition locks, graphical password schemes, pass face. All these methods have been

used by decades. Which may induce by hackers. It includes more disadvantages such as color code implemented for some servers only. So that secured server only enjoys the color code. Biometrics devices are used for security purpose, user can't able to carry the devices. In case of hacking admin could not able to track the type of hacker. Thus, the system is more vulnerable to the commonly identified threats [6, 7].

METHODOLOGY

According to SLAS in Online based Application having few main advantages and many disadvantages when it comes to weak single-factor authentication, which many are more familiar with as the single static passwords still employed by most companies. One advantage is that static passwords are easy to remember. When different systems have different passwords, they can be difficult to remember and may have to be written down, raising their vulnerability. One of the numerous drawbacks of single static passwords is how simple they are to crack. They're usually short and focused on topics that are personal to the individual, and they're usually just letters [8].

Static Method

The Internet's impact over the last few years has resulted in significant changes in how we access business systems. While the number of users requesting network access has increased, the network security barrier has disintegrated at all levels. Users' geographical locations have also broadened to the point that they can be anywhere in the world, not only in a different department or company branch office.

While increasing access has substantial productivity benefits, the security concerns have significantly increased. Authentication through the use of passwords was the traditional technique of securing system access. Traditional password security, unfortunately, is completely inadequate for securing the access requirements of today's scattered users. Businesses are still heavily reliant on user IDs and passwords to verify the identity of people attempting to access their systems, according to the DTI Information Security Breaches. Most businesses still utilize weak single factor authentication, which involves the usage of single static passwords. Static passwords have the advantage of being simple to remember. When you have multiple passwords for different systems, it becomes impossible to remember them all and they must be written down, making them susceptible. One of the numerous drawbacks of single static passwords is how easy they are to hack. They are often lettering only and are based on issues close to the user, such as birthdays, partner names, children's names, and so on. They're also subject to social engineering, which involves someone asking for or guessing your password. They are also detectable by spyware. Changing passwords on a regular basis is an alternate way of password management. When used properly, this has the advantage of being more secure than static passwords. Frequent password changes have the disadvantage of being easily forgotten, resulting in very high support expenses and dramatically increased administration expenditures. This is particularly relevant for larger organizations with hundreds of applications [9].

IMPLEMENTATION

In the following paragraphs we will learn more about how secure passwords are made and operated.

Login Authentication

In this project we provide a high security for password at users input level. Here the user while login every time must provide a password, a user defined image and must choose four different images which is given by the system. The user's password security is very much increased by giving various inputs scenarios while login into the system. This will prevent the attackers to view or modify the password and also attackers cannot login into system to misuse the users account. Before login into the system the user should create account by giving his/her details for accessing the account. During signup the user will input the details for their secured password and every time these factors are used for login (Figure 1).

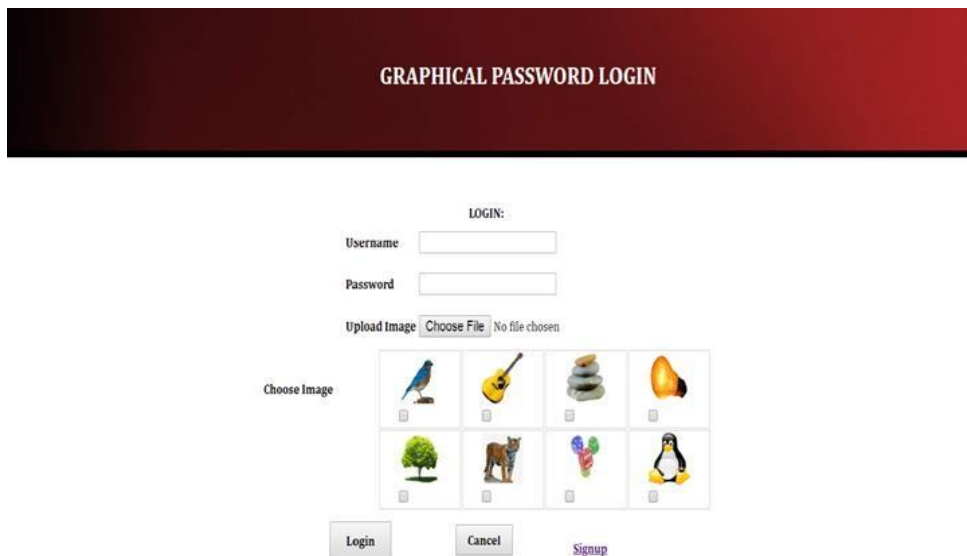


Figure 1. Login page.

Graphical Password Login

This module describes about how the user defined uploaded image works. The image uploaded by the user during signup is the image that he/she need to upload every time while login into system. The image can be with any format like .jpg, .png, .jpeg. Whenever the user uploads an image while login, the RGB value of the image currently uploaded will be verified with the image that was uploaded by the user during sign up. These two images RGB should match, so that the system accepts the user is an authorized user for login.

Graphical image shuffling: This is the password security where the image will get shuffled every time when the user login, that is the four images which was chosen by the user during sign up will be in any order in display while login. So the user must remember the images which was chosen during sign up but not the order of the image placed. These four images should match every time while the user login into the system. The system throws an exception to the user as unauthorized when even one of the images is chosen wrongly (Figure 2).



Figure 2. After login.

Graphical Image Shuffling

This is the password security where the image will get shuffled every time when the user login, that is the four images which was chosen by the user during sign up will be in any order in display while login. So, the user must remember the images which was chosen during sign up but not the order of the image placed. These four images should match every time while the user login into the system. The system throws an exception to the user as unauthorized when even one of the images is chosen wrongly.

Graphical password Updates

Here it explains about the changing the password, uploaded image and the chosen images. The system will have an option for updating the current password security level and the user can update the password whenever they need by logging into their corresponding account. When the user updated the security level of password the system will acknowledge the user that the password is updated successfully, and the user can be allowed to use the updated password during login (Figure 3).

Figure 3. Password update.

MATHEMATICAL CALCULATION

Each new calculation may be created from the past. The method of this type of algorithm, uses a one-way function (call it f). The one-time access system works by starting with an initial seed s , then generating passwords {
 $f(s)$,
 $f(f(s))$,
 $f(f(f(s)))$
 $\}$,
 ... as many times as necessary.

Each password is then dispensed in reverse, with $f(f(...f(s)))$ first, to $f(s)$.

After the set for s has been exhausted, a new seed value can be chosen if an indefinite succession of passwords is desired.

Lamport's method is used in the S/KEY one-time password system and its variant OTP.

An attacker who sees a one-time password may gain access for a limited time or login, but once that time period passes, the password is useless. To calculate the inverse function f^{-1} from the previous passwords, one must first develop a mechanism to calculate the next password in the series. This is incredibly tough to achieve because f was chosen to be one-way. If f is a cryptographic hash function, as is usually the case, the task is computationally infeasible (as far as we know). By supplying only a one-time password, the user can give the server with a static key for use as an encryption key in some mathematical algorithm schemes.

Users must respond to a challenge when using challenge-response one-time passwords. This can be accomplished, for example, by storing the token's created value within the token. To avoid duplicates, an extra counter is frequently used, resulting in separate one-time passwords if the same challenge is received twice. However, instead of applying both procedures, the computation normally does not use the prior one-time password. Instead of using time-synchronization, token-based methods of providing OTPs can employ one of these sorts of algorithms.

UNIT TESTING–MODULE WISE

Unit testing is to segregate each part of field in application and test that the individual parts are working in the given condition, and it test the login form by giving particular username and password of the admin (Figure 4) [10].

TEST CASE-LOGIN PAGE

SNO	TEST CASE-ID	TEST TYPE	STEP	TEST DESCRIPTION	EXPECTED RESULT	ACTUAL RESULT	RESULT
1	TC_01	Unit testing	User enters into application	Enter username & Password	Login accepted	System accepts the Process	Pass
2	TC_02	Unit testing	User enters invalid details	Enter username & Password	Login Not accepted	System not accepts the value	Failed
3	TC_03	Unit testing	If valid login	Displays master page for admin view and data input	Page viewed	Accept input	Pass

Figure 4. Test case-login page.

Functional Testing

Functional testing is used to test the admin whether all the requirements' fields such as respective input format. The main scope is to test the functional requirements; individual process is possible on functional testing on the entire system (Figure 5).

Integration Testing

Integration testing is done after unit testing, that is used to test whether the proper interface is provided (Figure 6).

TEST CASE_Key and User Creation

SNO	TEST CASE_ID	TEST TYPE	STEP	TEST DESCRIPTION	EXPECTED RESULT	ACTUAL RESULT	RESULT
1	TC_01	Functional testing	Create User	Input user details	Data stored in DB	System accepts the data and move to the next field	Pass
2	TC_02	Functional testing	Create Server	Input mail Details	Data stored in DB	System accepts the data and move to the next field	pass
3	TC_03	Functional testing	Generate details	Verify key	Data stored in DB	System accepts the details	pass

Figure 5. Test case key and user creation.

TEST CASE handshake process

SNO	TEST CASE_ID	TEST TYPE	STEP	TEST DESCRIPTION	EXPECTED RESULT	ACTUAL RESULT	RESULT
1	TC_01	Integration testing	Handshake process & data switch over to <u>other</u> server	Check formula and Calculation (For Warning)	Display available space	System accepts and show the available size of the server and current server	Pass

Figure 6. Test case handshake process.

CONCLUSION

In the future, safe digital audits research will try to verify the contents of a file system at a precise point in time.

A file system, for example, commits to the current version of its contents by delivering a MAC to a third-party. Using the MAC token, an auditor can check whether the file system still retains the old version at a later date. There has also been work on secure logging. In this work, a trusted machine writes encrypted logs that cannot be read or modified undetectably by an outsider. This work does not consider a large number of users concurrently accessing the data, there is no read and write access control (one key allows both read and write), the log is typically just appended and it is not optimized for writing in the middle, and a malicious outsider manipulating the order in which updates and reads are performed on the logging machine can compromise W and F. Moreover, in all this work,

the owner cannot convince a third party of some security violation. Current implementation of the logging client is loosely coupled with the operating system-based logging.

REFERENCES

1. Basak Bilgi, trBulent Tugrul," A Shoulder-Surfing Resistant Graphical Authentication Method" 2018 IEEE.
2. Bilal Eid Fayyadh, Khalid Mansour, Khaled W. Mahmoud," A New Password Authentication Mechanism Using 2D Shapes" 2018 8th International Conference on Computer Science and Information Technology (CSIT).
3. Chao Shen, Yufei Chen, Yao Liu and Xiaohong Guan," Adaptive Human–Machine Interactive Behavior Analysis With Wrist-Worn Devices for Password Inference"- IEEE Transactions On Neural Networks And Learning Systems.IEEE 2018.
4. Deepika Gupta,Dr. Vishal Goar, Akhand Pratap Singh,Shikha Mathur," Combination Of Textual And Graphical Based Authentication Scheme Through Virtual Environment"- 2017 IEEE.
5. K.Priya T.Venkaiah Naidu R.Vamsi Krishna ," An Advanced Information Security System Using Image Based Graphical Password Scheme"- 2nd International Conference on Trends in Electronics and Informatics (ICOEI 2018).
6. L.Gunaseeli, Dr.R.Aroul Canessane." GRAPHICAL PASSWORDS IMPLIES ON TOLERANCE PASSWORD, IMAGE CHOICE, AND PUZZLE LOGIN SECURITY"- international conference on information,communication & embedded systems (ICICES 2017).
7. Misbah Urrahman Siddiqui,Mohd. Sarosh Umar, Miftah Siddiqui," A Novel Shoulder-Surfing Resistant Graphical Authentication Scheme"- 2018 4th International Conference on Computing Communication and Automation (ICCCA), IEEE 2018.
8. Nida asmath," Conundrum – Pass: A New Graphical Password Approach. "-International conference on communication. IEEE 2019.
9. Noor Ashitah Abu Othman, Anis Shobirin Abdullah Sani, Muhammad Akmal Abdul Rahman, Fakariah Hani Mohd Ali," Directional Based Graphical Authentication Method with Shoulder Surfing Resistant"- 2018 IEEE Conference on Systems, Process and Control (ICSPC 2018), 14–15 December 2018, Melaka, Malaysia.
10. P. A. Sosa-Valles, J. G. Villalobos-Serrano, P. Velarde- Alvarado, V. García, J. R. Parra-Michel, L. Mena, R. Martínez-Peláez," My Personal Images as My Graphical Password"- IEEE Latin America Transactions, VOL. 16, NO. 5, MAY 2018.