

Graphical Password Authentication

Meher Gulhane, Amey Andurekar, Vaidehi Kute, Achal Maldhure, Sharwari Kale

Department of Computer Science Engineering, Sipna College of Engineering & Technology Amravati, Maharashtra, India

Professor A.V. Pande Department of Computer Science Engineering, Sipna College of Engineering & Technology Amravati, Maharashtra, India

Abstract - Graphical password is one of the techniques for authentication of computer security. Nowadays digital/computer security is the most important thing in computer science for protecting user or customer data. And Shoulder-surfing is one of the threats where a criminal can steal a password by direct observation or by recording the authentication session. There are several techniques available for this authentication, the most prevalent and simple of which is the Graphical password technique. So, we suggest a new approach to combat this problem. We have developed two concepts to combat shoulder surfing attacks. First, the user must register if the registration does not exist. Second, you must log in with a valid user ID and password. The password is a grouping of characters and numbers. Third, the user has to cross image-based authentication where the user can choose their password and this method has higher chances to offset each other. You should choose a password according to the registration password, it must match at login time. In color base authentication, there should be several color base passwords, and depending on the color, you need to remember the password sequence. And it's like three-factor authentication. So, here is proposed a new graphical password authentication technique that is resilient to shoulder surfing and also to other types of probable attacks.

Keywords: Graphical password, Authentication, Security, Text-based password, Recognition, Pictures

1. INTRODUCTION

Authentication is the process of determining that the person requesting a resource is the one who it claims to be. Most authentication system nowadays uses an integration of username and password. The problem with the password is that it requires the user to remember it and it should be kept secret. Each authentication system has its own guidelines and limitations like password length, password must contain alphanumeric and special characters. These passwords are mostly text-based passwords. Either user use passwords that are easy to remember like license plate numbers, parent names, phone numbers sometimes their own name which is very much predictable, or complex passwords that they overlook so they might be using the same password for different accounts or jot down their password somewhere. Moreover, the user is vulnerable to various attacks. Text-based passwords face security and usability matters.

To overcome these shortcomings of alphanumeric passwords, graphical password schemes have been proposed. In a graphical password authentication application by using the 6 passports scheme a password contains an image where the user can input the password with the help of mouse events like click and drag. Picture Superiority Effect Theory reveals that pictures can be recognized and recalled easily by the human brain, enhancing the ability to Strong passwords can be invented which are resistant to guessing, dictionary attack, and social engineering.

1.1 Problem Statement

An alphanumeric password is an old traditional common authentication method. Practically this traditional method is a too insecure system. For example, an attacker may choose an easily guessed user's password, if a user is not using a strong password. Users may use the same password for multiple devices or sites. These are all insecure characteristics for normal users. And authentication is one of the important security points where the user has active responsibility for their personal information security. If we use the old traditional password system then there may have the possibility of to dictionary attack, Brute Force Attack.

1.2 Objective

- i. To design a Graphical Password Authentication implemented in the mobile application.
- ii. To implement the Graphical Password Authentication application using the PassPoint technique

2. LITERATURE REVIEW

[1] In Dec 2021 author H. Gao proposed a graphical password scheme using color login. In this color, login uses a background color which decreases login time. The possibility of accidental login is high and the password is too short. The system developed by Sobrado is improved by combining text with images or colors to generate session passwords for authentication. Session passwords can be used only once and every time a new

4. CONCLUSION

Digital devices are becoming part of our life day by day. By using digital devices, we have able to know about the authentication process. Validation is an integral part of security. Authentication will give the customer greater security. Specific review articles research in the same field about the specific assaults found during validation. Printed hidden-term authentication is an excellent testing device. It is more useful and secure compared to previous old base graphical password authentication systems. Since the password space is very large, it offers security against brute-force attacks. It's easy to use. Passwords can be easily created and recalled. The randomization in both authentication systems provides strong security against shoulder surfing. To have a good system, you need high security and good usability, and can't be separated them. Shoulder navigation attack is subject to safety precautions. However, the proposed methods for the shoulder surfing problem still need to be improved. This system can also be used to add a higher level of security to the text-based password system. This system is very cheap compared to a biometrics system.

5. REFERENCES

- [1] Dec 2020, H. Gao proposed a paper on a "graphical password scheme using color login".
- [2] In May 2021, M. Sreelatha proposed Hybrid Textual Authentication Scheme.
- [3] Er. Aman Kumar, Er. Naveen Bilandi, Department of Computer Science and Engineering, DAV University, Jalandhar, Punjab, India "Graphical Password-Based Authentication Based System for Mobile Systems".
- [4] Miss.Swati Tidke, Miss Nagama Khan, Miss.Swati Balpande Computer Engineering, RTM nagpur university, M.I.E.T Bhandara, "Password Authentication Using Text and Colors".
- [5] Veena Rathanaivel, Swati Mali, Student M. Tech, Department of Computer Engineering, K J Somaiya, College of Engineering Mumbai, "Graphical Password as an OTP".
- [6] Veena Rathanaivel, Swati Mali, Student M. Tech, Department of Computer Engineering, K J Somaiya, College of Engineering Mumbai, "Graphical Password as an OTP".
- [7] In 2021 Aayush Dilipkumar Jain, Ramkrishna Khetan Krishnakant Dubey, Prof. Harshali Rambade K. Elissa, Department of Information Technology Vidyalkar Institute of Technology, Mumbai, "Color Shuffling Password-Based Authentication".