A Comprehensive Survey on Graphical Password Authentication System

Dr.THOMAS FELDMAN

[1]*Final Year PG Student, Dept of MCA, School of CS & IT, Jain Deemed-to-be University, Bengaluru*

[2]*Professor, Dept of MCA, School of CS & IT, Jain Deemed-to-be University, Bengaluru*

Abstract

In this paper, we are focusing on the concept of graphical password authentication system. Graphics indicate photographs, design patterns and may other image format, and password means combination of alphabetical latter, symbol, numbers used to prove the identification of a user during the authentication process. And authentication is a procedure of recognizing a user's identity. Graphical password is one of the alternative solutions to text-based password. The graphical passwords are attractive, and our human brain usually remember image better than words. As we know that our human memory or human brains has remarkable memory capabilities to recognize and recall visual images. Most of the time we used alphanumeric password, but these alphanumeric passwords are easy to crack through different types of attack. In this project, you have to choose password according to register password, it's need to match. And there should be several color base passwords and according to color you have to remember the sequence of password. And it's like three-factor authentication. To prefer system is used to decrease the shoulder surfing attack, dictionary attack, and it's easy to remember, and it will upgrade the security of existing Application.

Keyword-Computer Authentication, Computer security, Graphical Password.

1 INTRODUCTION

Authentication is like a security doorkeeper for computer systems. And Graphical passwords are one of the methods of authentication in computer security. Now days all users are want simple authentication which will very easy to remember and easy to use for authentication. Graphical passwords hold human memory has outstanding memory potentiality to acknowledge and recall visual images. graphical password or colour base password, a user can register random and secure password and there don't have any troubled the registered password. Authentication is a data access point that manages consumer security assurance. It is a process that grants in a particular context requiring the customer to. Validation schemes are categorized as token-based authentication, validation based on biometrics, validation based upon knowledge. Tokens are used as a Hidden Key in token-based authentication. Graphical password, numerous forms of pictures or shapes and colours are used as password. Also, psychological researcher says that pictures may be simply remembered by human brain instead of text. Attributable to this human characteristic, graphical passwords are superior to textual passwords. As we all know that images base password is resistant of dictionary attack, keylogger, social engineering and so on.

User is bestowed with a group of random images and random sequence of colour password throughout registration. The user should choose the actual image from this set as a password. Throughout authentication, user has to establish those preselected pictures in an exceedingly correct sequence. Graphical passwords techniques are classified into 2 types: recognition-based and recall based graphical techniques. In recognition-based techniques is authenticated by tight him to identify one or additional images he chooses during the registration stage. In recall-based techniques is asked to replicate something that he created or chosen earlier throughout the registration stage.

2. LITERATURE SURVEY

"Graphical Password Authentication" by Shraddha M, Leena S. Gawade, Prathamey K. Rane. [1]

They designed a graphical password technique wherever they have presented some of impotent technic of graphical password for example multiple-image base password that some number of pictures can offer to user and that they need to select one or more of them. Next grid base scheme, which is easy object there aren't any further displays are required. Next Triangle scheme, which is provide with protrusive surface and numbers of images shown are virtually same, it's tough to choose out. Then Hybrid textual authentication, during this methodology colors are already given user solely have to bear in mind the sequence. And it is very simple to assign no special algorithm. Signature based scheme that will not be derived because it is and little mistake in signature can denied the access. Most impotent things in this paper is that calculate base of username. So, this is often new scheme provides solves the numerous issues of existing system.

"Enhancement of Password Authentication System Using Graphical Images" by Amol Bhand, vaibhav desale, Swati Shirke, Suvarna Pansambal.[2]

In this paper mainly focuses on the construct of graphical password system completely with different authentication systems. And also, the basic goal of this method is to attain higher security with easy technique to use by a user and more durable to guess by hacker. So, they develop 3 different kind of authentication system A. Pass point, B. Cued Click Point,

C. Persuasive Cued Click Points.

Pass point, during this system user should choose 5 points from single picture and at the time of choosing and through the time of login user has to repeat identical sequence of the points from single image. And Cued click point has the same construct as of the pass point however the most distinction between them is passing 5 points on five completely different image one point per image. PCCP could be a authentication technic. PCCP is a best technology but it has security issues connected with it.

"A New Graphical Password Scheme Resistant to Shoulder-Surfing" by Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu, Uwe Aickelin.[3]

In this paper they are discuss about security features of graphical authentication. Different graphical password schemes have different techniques to scale back the cyber-attacks. As you recognize that graphical password is simple to remember and high usability with high security. So graphical password schemes are provided higher security than text -based passwords. Some of the resistance of graphical password authentication attacks are shoulder surfing, brute force, dictionary attacks, guessing attack, spyware and social engineering attacks. During this paper they supply a quick description and classification of various graphical password schemes followed by information about vulnerabilities within various schemes and suggestions for future development.

"The Shoulder Surfing Resistant Graphical Password Authentication Technique" by Mrs.Aakansha S. Gokhalea, Prof. Vijaya S. Waghmareb.[4]

In this paper mainly focuses on Authentication, Graphical Password, Security and Shoulder surfing. Simple way of authentication is that the method of verifying the identity of someone or device. A graphical password is a form of authentication using images or colour rather than letters, digits or special characters. And shoulder surfing is a type of attack which refers to looking over shoulder or possible to see their credential data such as password, PIN and others sensitive information. They gave brief overview of authentication technique like recognition, recall base techniques, Image Pass techniques, Colour Login techniques etc. Overall, they develop a system which is resistant to all alternative possible attacks and this method may be used for extremely secure systems.

"Minimizing Shoulder Surfing Attack using Text and Colour Based Graphical Password Scheme" by Prof. S. K. Sonkar, Prof. R. L. Paikrao, Prof. Awadesh Kumar.[5]

In this paper they develop a system that uses text and color-based graphical password which is useful in reducing the shoulder surfing attack. This theme are usable anyplace and anytime with a low error rate and faster authentication result. This scheme can take pleasure in the argument that people recognize images better and are easier to remember. In this system, it will provide a strong line of defense against shoulder surfing brute force, intersection and educated guess attacks. By using this scheme, the user can effectively access the system. They have planned to reduce the Shoulder surfing attack and it can improve the protection of existing applications.

"A Graphical Password Against Spyware and Shoulder-surfing Attacks" by Elham Darbanian, Gh. Dastghaiby fard.[6]

In this document focuses on graphical passwords, Spyware attacks, and shoulder-surfing attack. This scheme is largely resistant to spyware. Shoulder-surfing attacks include mouse clicks, touch screens, or light pens. Using the keyboard is more secure than using the mouse. The scheme

proposed in this document is secure against shoulder surfing attack.
So, if we click or touched directly on image then it possible to attack for shoulder surfing. So, they develop a scheme to used keyboard to select image base password. In this scheme, they explain about different login phases in order to understand the character of images, which is time-consuming and costly.

"Text based Graphical Password System to Obscure Shoulder Surfing" by Khazima Irfan, Agha Anas, Sidra Malik, Saneeha Amir.[7]
In this article, they have implemented a text-based graphical password project for an android application using android studio. They focus on graphical password, password authentication app, mobile framework, shoulder surfing and android. To create passwords that are memorable and less vulnerable to shoulder surfing. And they provide a graphical password scheme for text-based movable frame. They compared the traditional graphical password system to movable text-based graphical images. In this system, they develop the registration phase, the login phase, the movable frames and the Android implementation. In this document, they gave a solution based on text-based graphical password techniques. To build this project, they used android studio and android application. They implement a scheme of graphical password system with multiple character, images for avoiding the dictionary attacks. So this paper was really help to know about different authentication for android system.

"A Shoulder-Surfing Proof Graphical Password Authentication for Mobile Devices" by Teoh joo Fong, Azween Abdullah, NZ Jhanjhi.[8]
In this paper, they specialize in Mobile graphical password for mobile device. And they focus on multi-elemental passcode, shoulder-surfing proof passcode and mobile authentication model. Therefore, they are developing mobile graphical password authentication, which works as a quick password security mechanism for mobile devices. Currently, most mobile devices are using six-pin numeric password authentication, which is extremely vulnerable to shoulder-surfing attacks and spyware attacks. They offer a graphical multi-element password authentication model for mobile devices. And the multi-elemental graphical password is resistance-shoulder surfing attacks and spyware attacks. In this paper, they discuss the "Coin passcode". Coin passcode is a model that uses multiple elements found in the structure of any coin. In coins from different countries, there are always a combination of symbols, different numerical values and a few words. The Coin Passcode is designed to overcome the vulnerability of shoulder surfing attack and is currently designed specifically for swift mobile authentication. The coin password is higher password complexity and overcome from shoulder surfing attacks and other vulnerability for mobile device.

"Security in Graphical Authentication" by Robert G. Rittenhouse, Junaid Ahsenali Chaudry and Malrey Lee.[9]
In this paper they focus on computer security of authentication. As we know that authentication is the gatekeeper for computer systems. Graphical password is one of the techniques for authentication system. Graphical authentication is resistance of cyber-attack like social engineering, brute force attacks, shoulder surfing attack. In this paper they propose of different graphical password schemes, for example text-based password, image base password, colour base password, biometric base etc. The main reason for graphical password authentication is that people remember images better than text. Therefore, the graphical password is a password which is easy to remember and more secure passwords to produce and which reduces the temptation for users to create insecure passwords.

In this paper they analyse of possible security attacks or graphical password attack likes shoulder surfing, brute force attacks, guessing attacks, dictionary attacks, spyware and social engineering attacks.
Shoulder surfing: shoulder surfing is a type of attack which refers to looking over shoulder or possible to see their credential data such as passcode, PIN, password and others credential information. Most graphical authentications are generally more vulnerable to shoulder-surfing attacks than text-based passwords, but some graphical authentication methods are designed to resist the shoulder surfing attack.
Brute Force Attacks: it is a one type of attack where the hacker tries to guess possible combination password and used to crack the main password. graphical authentication schemes are one type of technic to defend against brute force attack.

3. CONCLUTION

This document focuses primarily on the concept of graphical password authentication system. This is a security base project. In this project I design three type of authentication system text-based authentication, Colour-base authentication and image base authentication. In this survey paper, I have preferred 9 research papers, which is help me internal or externally guide to build my project and research paper. Some of the research papers are really help me to build my project and to gain strong knowledge. I have learned different papers and get to know different technique. In this throw of survey, I studied on more than 10 graphical password design and 4 algorithms. And some of the security methodology like avoiding shoulder surfing, resistance of brute force attacks.
Graphical password is one of the most authentication technics, which can use mobile application or desktop application or anywhere. The purpose to build this graphical password are easy to use, easy to remember and more attractive form text base password. Graphical password techniques which are avoid shoulder surfing attack, brute force attack, social engineering attack. There are possibilities for future research to develop new authentication techniques that avoids above possible attacks.

4. REFERENCE

[1] ShraddhaM. Gurav, Leena S. Gawade, Prathamey K. Rane, Nilesh R. Khochare " Graphical Password Authentication.", 2014 IEEE;

[2] Amol Bhand, Vaibhav desale, Swati Shirke, Suvarna Pansambal "Enhancement of Password Authentication System Using Graphical Images",International Conference on Information Processing (ICIP) Vishwakarma Institute of Technology, Dec 16-19, 2015;

[3] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu, Uwe Aickelin "A New Graphical Password Scheme Resistant to Shoulder-Surfing";

[4]. Mrs.Aakansha S. Gokhalea , Prof. Vijaya S.Waghmareb, "The Shoulder Surfing Resistant Graphical Password Authentication Technique", Published by Elsevier B.V, 2016.03;

[5] Prof. S. K. Sonkar, Prof. R. L. Paikrao , Prof. Awadesh Kumar, Mr. S. B. Deshmukh "Minimizing Shoulder Surfing Attack using Text and Colour Based Graphical Password Scheme", February - 2014;

[6] Elham Darbanian , Gh. Dastghaiby fard "A Graphical Password Against Spyware and Shoulder-surfing Attacks", International Symposium on Computer Science and Software Engineering, jun-2015;

[7] Khazima Irfan, Agha Anas, Sidra Malik, Saneeha Amir "Text based Graphical Password System to Obscure Shoulder Surfing",13th January-2018;

[8] Teoh joo Fong, Azween Abdullah, NZ Jhanjhi, Mahadevan Supramaniam "A Shoulder-Surfing Proof Graphical Password Authentication Model for Mobile Devices", International Journal of Advanced Computer Science and Applications, Vol. 10, No. 1, 2019;

[9] Robert G. Rittenhouse, Junaid Ahsenali Chaudry and Malrey Lee "Security in Graphical Authenticatio", International Journal of Security and Its Applications Vol. 7, No. 3, May, 2013;

[10] Ahmad Almulhem, "A Graphical Password Authentication System", May-24,2020;

[11] Sanjay E. Pate & Bhojaraj H. Barhate "A survey of Possible Attacks on Text & Graphical Password Authentication Techniques", International Journal of Scientific Research in Survey Paper Computer Science and Engineering, Vol.6, Special Issue.1, pp.77-80, January- 2018;

[12] Lip Yee Por, Lateef Adekunle Adebimpe, Mohd Yamani Idna Idris & Chee Siong Khaw and Chin Soon Ku, "LocPass: A Graphical Password Method to Prevent Shoulder-Surfing", 8 October 2019