Graphical Authentication System Using Pass Matrix

Sarojini [1], Priya [2], Bhuvaneshwari [3]
[1,2,3,]*Students Member, Department of Computer Science and Engineering*
AVC College of Engineering ,Mannampandal

Abstract

Authentication based password is largely used in the computer security and privacy. Most of the traditional passwords are numbers and alphabets character. That can be easily identified by the unauthorized people. The identification leads the shoulder surfing attacks. However, human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as"the weakest link" in the authentication chain. With web applications and mobile apps piling up, people can access these applications anytime and anywhere with various devices. To overcome these problems we introduce a novel authentication system called PassMatrix resist shoulder surfing attacks.

Keywords**:** *Graphical Passwords, Authentication, Shoulder Surfing Attack***.**

Problem Definition

Textual passwords have been the most widely used authentication method for decades. Comprised of numbers and upper- and lower-case letters, textual passwords are considered strong enough to resist against brute force attacks. However, a strong textual password is hard to memorize and recollect.Therefore, users tend to choose passwords that are either short or from the dictionary, rather than random alphanumeric strings.Various graphical password authentication schemes were developed to address the problems and weaknesses associated with textual passwords.

Proposed System

Secure graphical authentication system named PassMatrix is offered that protects users from becoming fatalities of shoulder surfing attacks when inputting passwords in public through the usage of one-time login indicators. A login indicator is randomly generated for each pass-image and will be useless after the session terminates. The login indicator provides better security against shoulder surfing attacks, since users use a dynamic pointer to point out the position of their passwords rather than clicking on the password object directly.

Literature Survey:

[1] Crypt analysis of password authentication scheme

Author: - S. Sood, A. Sarje, and K. Singh

Description

The password authentication systems heve was increasing in recent years. System is still weak to server attack and stolen smart card attack. Also , a password change protocol of the system is neither suitable to users nor low efficient. There is no handy data can be gained from the values kept in smart cards. To prevent server attack, we suggest transferring a user authentication operation from servers to a registration centre, which can guarantee every, has another private key.

[2]Graphical password authentication: cloud securing scheme

Author: - S. Gurav, L. Gawade, P. Rane

Description

Graphical password is one of the alternative solutions to alphanumeric password as it is very tedious process to remember alphanumeric password. When any application is provided with user friendly authentication it becomes easy to access and use that application. One of the major
reasons behind this method is according to psychological studies human mind can easily remember images than alphabets or digits. In this paper we are representing the authentication given to cloud by using graphical password. We have proposed cloud with graphical security by means of image password. We are providing one of the algorithms which are based on selection of username and images as a password. By this paper we are trying to give set of images on the basis of alphabet series position of
characters in username. Finally cloud is provided with this graphical password
authentication

[3] Deja vu: A user study using images for authentication

Author:-R. Dhamija and A. Perrig

Description

Current secure systems suffer because they neglect the importance of human factors in
security. We address a fundamental weakness of knowledge-based authentication schemes, which is the human limitation to remember secure passwords. Our approach to improve the security of these systems relies on *recognition-based*, rather than *recall-based* authentication. We examine the requirements of a recognition- based authentication system and propose
Déjà Vu, which authenticates a user through her ability to recognize previously seen images. Déjà Vu is more reliable and easier to use than traditional recall-based schemes, which require the user to precisely recall passwords or PINs. Furthermore, it has the advantage that it prevents users from choosing weak passwords and makes it difficult to write down or share passwords with others.

[4] Design and analysis of graphical passwords
Author: - J. Jermmyn, A. Mayer, F. Monrose
Description:

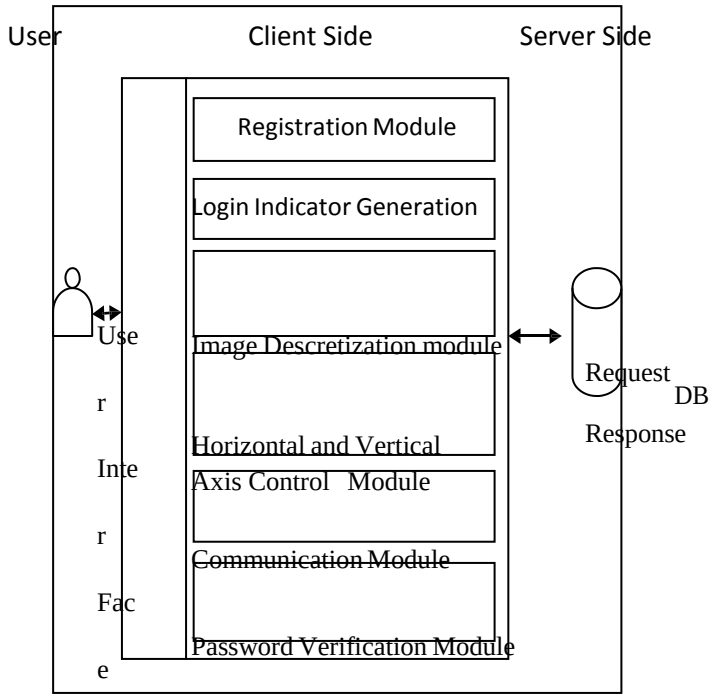
The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, some researchers have developed authentication methods that use pictures as passwords. In this paper, I conduct a comprehensive survey of the existing graphical password techniques. These techniques into two categories: recognition- based and recall-based approaches. I discuss the strengths and limitations of each method and point out the future research directions in this area. I also developed three new techniques against the common problem exists in the present graphical password techniques. In this thesis, the scheme of each new technique will be proposed; the advantages of each technique will be discussed; and the future work will be anticipated.

[5] Pass points: Design and longitudinal evaluation of graphical password system
Author:-S. Wiedenbeck, J. Waters, J. Birget

Description

The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, some researchers have developed Authentication methods that use pictures as passwords. In this paper, I conduct a comprehensive survey of the existing graphical password techniques. I classify these techniques into two categories: recognition-based and recall-based approaches. I discuss the strengths and limitations of each method and point out the future research directions in this area. I also developed three new techniques against the common problem exists in the present graphical password techniques. In this thesis, the scheme of each new technique will be discussed; and the future work will be anticipated.

Architecture



OVERVIEW OF THE PROJECT

- Registration Phase
- Image Discretization Module
- Horizontal and Vertical Axis Control Module
- Login Indicator generator Module
- Communication Module
- Password Verification Module

Registration phase

User creates an account which contains a username and a password.The user has to choose images from a provided list as pass- image. Then the user will pick a pass-square or each selected pass-image from the grid, which was divided by the image discretization module. The user repeats this step until the password is set.

Image Discretization Module

This module divide each image into square, from which users would choose one as the pass-square.An image is divided into a 7 x11 grid. The smaller the image is discretized, the larger the password space.

Horizontal and Vertical Axis Control Module

It consists of two bars that are that are horizontal bar and vertical bar. Horizontal bar for sequence of letters and vertical bar
for sequence of numbers. This control module provides two functions Drag and Filling functions for users to control both bars and both bars are circulative. These bars are implicitly point out the location of the user's pass square.

Login Indicator generator Module

These modules describe when the user login the section each time login indicator will generate random ID with letters and numbers during authentication phase**.** The

generated login indicator can be given to users visually or acoustically.

Communication Module

Communication module is the in charge of all the information transmitted between the client devices and authentication server. It enables the communication to the authenticated phases it generally happened client side and authentication server side.

Password Verification Module

This module verifies the user password during the authentication phase. A pass square acts similar to a password digit in the text-based password system. The user is authenticated only if each pass-square in each pass-image is correctly aligned with the login indicator. The details of how to align a ogin indicator to a pass-square will be described in the next section.

Conclusion

In order to protect users' digital property, authentication is required every time they try to access their personal account and data. However, conducting the authentication process in public might result in potential shoulder surfing attacks. Even a complicated password can be cracked easily through shoulder surfing. Using traditional textual passwords or PIN method, users need to type their passwords to authenticate themselves and thus these passwords can be revealed easily if someone peeks over shoulder or uses video recording devices

such as cell phones. To overcome this problem, we proposed a shoulder surfing resistant authentication system based on graphical passwords, named Pass Matrix. Using a one-time login indicator per image, users can point out the location of their pass- square without directly clicking or touching it, which is an action vulnerable to shoulder surfing attacks.

REFERENCES

[1] Sood, A. Sarje, and K. Singh, "Crypt analysis of password authentication schemes: Current status and key issues, "in methods and models in computer science, 2009. ICM2CS 2009. Proceeding of International conference on, Dec 2009, pp. 1-7.

[2] S. Guru, L. Gawade, P. Rane, and N. khochare, "Graphical Password Authentication: Cloud Securing Scheme, "In Electronical Systems, Signal Processing and computing technologies (ICESC), 2014

[3] L.Jermyn, A. Mayar, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords".

[4] R. Damija and A. Perrig, "Déjà vu: A user study tha image for authentication,"in proceeding of the 9th conference on USENIX Security Symbosium-Volume 9.

[5] S.Widenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon,"Passpoints: Design and longitudinal evaluation of graphical password system".

[6] A. Paivio, T. Rogers, and P. Smythe, "Why are pictures easier to recall than words?" Psychonomic Science, 1968.

[7] D. Nelson, U. Reed, and J. Walling, "Picture superiority effect," Journal of Experimental Psychology: Human Learning and Memory, vol. 3, pp. 485–497, 1977.

[8] S. Brostoff and M. Sasse, "Are pass faces more usable than passwords? a field trial investigation," PEOPLE AND COMPUTERS, pp. 405–424, 2000.

[9] A. De Angeli, M. Coutts, L. Coventry, G. Johnson, D. Cameron, and M. Fischer, "Vip: a visual approach to user authentication," in Proceedings of the Working Conference on Advanced Visual Interfaces. ACM, 2002, pp. 316–323.

[10] S. Brostoff and M. Sasse, "Are pass faces more usable than passwords? a field trial investigation," PEOPLE AND COMPUTERS, pp. 405–424, 2000. [11] A.

[12] B. Ives, K. Walsh, and H. Schneider, "The domino effect of password reuse," Communications of the ACM, vol. 47, no. 4, pp. 75–78, 2004.

[13] J. Long and K. Mitnick, No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Elsevier Science, 2011.

[14] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human adversaries are more powerful than expected,"