AN IMPROVED AUTHENTICATION SYSTEM RESISTANT TO SHOULDER SURFING ATTACK

AUTHORS:Dr. REKHA PATIL, SUSHMITA PATIL

ABSTRACT

Authentication based on passwords is widely used in applications for computer security and privacy. However, human actions such as choosing bad passwords and inputting passwords in an insecure way are considered as the weakest link in the authentication chain. Rather than arbitrary alphanumeric strings, users tend to choose passwords either short or meaningful for easy memorization. With web applications and mobile apps piling up, people can access these applications anytime and anywhere with various devices. This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users credentials. To overcome this problem, we proposed a novel authentication system Pass Matrix, based on graphical passwords resisting shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, Pass Matrix offers no hint for attackers to figure out or narrow down the password even when they conduct multiple camera-based attacks. We also implemented this work in real time by using cloud computing.

Index Terms — Graphical passwords authentication, shoulder surfing attack.

Introduction

Cloud Computing Issues & Challenges – Cloud computing is a common term you hear about on and off. And professionals use it without even knowing about the actual concept. So to put it in simple words, cloud computing is storing, accessing, and managing huge data and software applications over the internet. In this technology the entire data is secured by firewall networks. You can use the software without using your computer 's hard drive as the software and data is installed in world wide data centers.

The cloud technology is used by many people in their daily lives. Using web based email services or preparing any document over the internet is a common example of the cloud technology. In the IT industry, there are three different types of cloud computing such as infrastructure as a service (IaaS), platform as a service (PaaS), Software as a service (SaaS). All these types of cloud technologies are being used for the different kind of services. Cloud technology is very useful in business development as it brings astonishing results in a timely manner.

However, there is a minor gap between the success and failure in businesses. Selection of the right technology takes your business to new heights while a few mistakes land your business in troubles. Every technology comes with a baggage of some pros and cons. Similarly, cloud computing too comes with its share of issues despite being core strength of some business industries. It also can create some major problems under some rare circumstances. issues and challenges of cloud computing are featuring as ghosts in the cloud. Let us talk in brief about some real life ghosts of cloud computing.

Data Security Concern

When we talk about the security concern of the cloud technology, then a lot of questions remain unanswered. Multiple serious threats like virus attack and hacking of the client 's site are the biggest cloud computing data security issues. Entrepreneurs have to think on these issues before adopting cloud computing technology for their business. Since you are transferring your company 's important details to a third party so it is important to ensure yourself about the manageability and security system of the cloud.

Selecting the perfect cloud setup

Choosing the appropriate cloud mechanism as per the needs of your business is very necessary. There are three types of clouds configuration such as public, private, and hybrid. The main secret behind successful implementation of the cloud is picking up the right cloud. If you are not selecting the right cloud then maybe you have to face some serious hazards. Some companies having vast data so they prefer private clouds while small organizations usually use public clouds. A few companies like to go for a balanced approach with hybrid clouds. Choose a cloud computing

consulting service which is aware and clearly disclose the terms and conditions regarding cloud implementation and data security.

Real time monitoring requirements

In some agencies, it is required to monitor their system in real time. It is compulsory term for their business which they continuously monitor and maintain their inventory system. Banks and some government agencies need to update their system in real time but cloud service providers are unable to match this requirement. This is really a big challenge for cloud services providers. As the TEXTUAL passwords have been the most widely used authentication method for decades. Comprised of 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. Based on some studies such as those in humans have a better ability to memorize images with long-term memory (LTM) than verbal representations. Image-based passwords were provided to be easier to recollect in several user studies As a result, users can set up a complex authentication password and are capable of recollecting it after a long time even if the memory is not activated periodically. The human actions such as choosing bad passwords for new accounts and inputting passwords in an insecure way for later logins are considered as the weakest link in the authentication chain. Therefore, an authentication scheme should be designed to overcome these vulnerabilities. In this paper, we present a secure graphical authentication system named Pass Matrix which protects users from becoming victims 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. Improved graphical password resistant to shoulder-surfing using 4-way recognition-based sequence reproduction (RBSR4)

Graphical passwords seem to be the solution as it is described in more paper. A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). Despite the high standards of graphical passwords, they are still vulnerable to some kinds of attacks. Authors is a new graphical password scheme that takes advantage of graphical input displays to achieve better security than text-based passwords. The proposed research is an approach to enhance the existing graphical password techniques and resist against the shoulder surfing. This system can be improved to provide a wider password space if more server variables are involved (such as date). Study on robustness of the system against sniffing can be suggested for further study.

2. Zhi Li; Qibin Sun; Yong Lian; D.D. Giustoan Association-Based Graphical Password Design Resistant to Shoulder-Surfing Attack

In line with the recent call for technology on Image Based Authentication (IBA) in JPEG committee [1], authors have presented a novel graphical password design in this paper. It rests on the human cognitive ability of association-based memorization to make the authentication more user-friendly, comparing with traditional textual password. Based on the principle of zero-knowledge proof protocol, they further improve our primary design to overcome the problem of shoulder-surfing attacks without adding any extra complexity into the authentication procedure. System performance analysis and comparisons are presented to our proposals.

3.C. Cullen Inherent vulnerabilities of one-time passcode mechanisms

Traditional user identification and authentication mechanisms are no longer considered adequate due to the sophistication of hackers and hacker tools. The one-time passcode mechanism is becoming commonly used. However, these mechanisms do have vulnerabilities that should be considered when evaluating a product. This paper covers two vulnerabilities, a passive attack used when a one-time passcode card is in two databases and an active attack of masquerading as a one-time passcode server to steal the information to be able to masquerade as a user.

4.Adrian-Viorel Diaconu Passcode Based Authentication Protocol: Part I

This article aims at presenting a method for implementing an authentication protocol, which combines the two basic schemes (something known to the user or something owned by him), efforts were focused on highlighting the elements of software design and the basic procedures of the proposed authentication system Also, an

assessment is made on strength of passcode by quantifying the average tims

scrolling passcodes space to reach a specific combination. Taking into account that the criteria are “worst case scenario” type (for this kind of evaluation) in the following are proposed and evaluated two methods for enhancing / increasing the average time scrolling the space, one of them being implemented in the case of the presented authentication scheme. If in this first part of the paper software implementation, performance and security issues are discussed, in the second part (which will be published in the next issue of the journal) will be dealt with topics related to hardware implementation.

5. Vishwanath Ullagaddi; Firas Hassan; Brent D. Cameron; Douglas Nims; Vijay DevabhaktuniA new passcode based approach for hiding classified information in images

This paper proposes a method of hiding classified data in images based on three different levels of security. Instead of hiding data directly, pixels are randomly selected and their higher nibble bits are matched with the data bits. A two bit code (2BC) is generated to encode the location of the matching bits. The two bit code is embedded in the image based on a password using three different suggested techniques. The three different levels of security make this method highly difficult to intercept and useful for secure open channel communications.

6. Yong-Zhang Luo; Cheng Zheng; Chenglian Liu; Biying Zhao A Dynamic Passcode System for Mobile Purchasing without Bank Card

Credit cards use a security system where the personal identification number (PIN) is a constant. This presents a security vulnerability as this gives the attacker more time to find the PIN and defraud the bank.In this paper the authors proposed a scheme that is based on a security code that is dynamic, that is, the code will change every time the mobile device is used for a purchase. This system will not require more hardware, but rather, a few more lines of software. We believe both consumers and banks will welcome the new system because it will eliminate the expense of a bank card by becoming a smart phone application. We also think that the increase in security from the software will greatly outweigh the extra cost of the software required for the system.

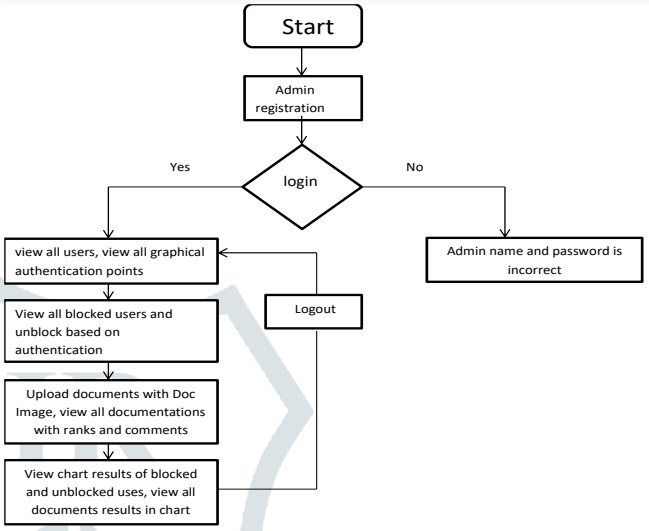
SYSTEM DESIGN

1. ADMIN

2. USER

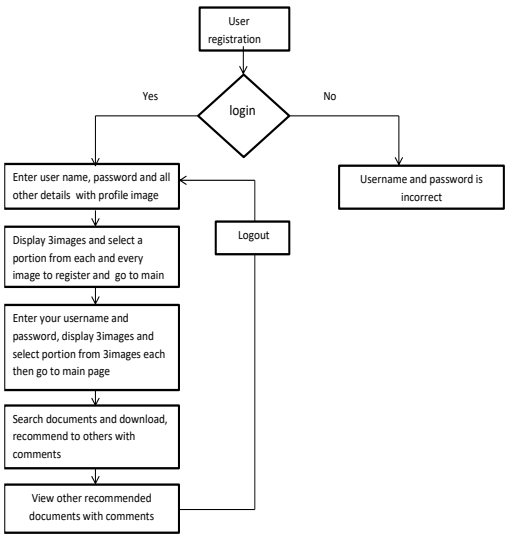
1. ADMIN

In this module, admin has to login with valid username and password. After login successful he can do some operations such as view all users, their details and authorize them, View all users graphical authentication points, view all blocked users (who tried wrong graphical authentication points 3 time), View unblock requests and unblock them, upload Documents with image and view all uploaded documents with rank and comments of it, View users results based on number of users active and blocked, View the documents based on rank.



2. USER

In this module, there are no numbers of users are present. User should register before doing some operations and also set graphical authentication points while registration. After successful registration he can login by using valid user name and password and also graphical authentication points. Successful login He will do some operations like view profile details, Chang graphical authentication points, search documents and download / View and comment on it / recommend it to others, View all recommended documents.



MODULAR DESCRIPTION

1. Multi Layer Image Authentication
2. Grid Image Authentication
3. Color Image Authentication
4. Random Guess Attack
5. Login / Register
6. Upload Image
7. View Status
8. View Requests
9. Approve / Cancel

1. Multi Layer Image Authentication To overcome the security weakness of the traditional PIN method, the easiness of obtaining passwords by observers in public, and the compatibility issues to devices, we introduced a graphical authentication system called Pass Matrix. In Pass Matrix, a password consists of only one pass-square per pass-image for a sequence of images. The number of images (i.e., n) is user-defined. Below figure1 demonstrates the proposed scheme, in which the first pass-square is located at the first image, the second pass-square is the top of the smoke in the second image third image. In Pass Matrix, users choose one square image for a sequence of n images. Based on the user study of Cued Click Points. CCP method does a good job in helping users recollect and remember their passwords. If the user clicks an incorrect region within the image, the login will be failed.

Fig 1: A password contains three images(n=3) with a pass square in each. The pass square are as shown in the orange-filled area in each image.

2. Grid Image Authentication

In this type of authentication multiple images can be provided to the user, the user has to select the image that he can to log in, this will provide more security (as shown in the fig 2).

Fig 2:(a) The main page of PassMatrix, users can register an account, practice or start to login .(b) Users can choose from a list of images as their pass images.(c) There are 7x11 squares in each image, from which users choose one as the pass-square.

3.Color Image Authentication

In this type the authentication is user by the color coordinates of that position. In normal Authentication the password is set according to the region. But in this type of authentication we choose the color coordinates for the password setting

4. Random Guess Attack

To perform a random guess attack, the attacker randomly tries each square as a possible pass-square for each pass image until a successful login occurs. The key security determinants of the system are the number of pass-images and the degree of discretization of each image. To quantify the security of Pass Matrix against random guess attacks, we define the entropy of a password as in equation (1). The table defines the notations used in the equation (1). If the entropy of a password space is k bits, there will be 2kpossible passwords in that space.

Entropy = log2 ((Dx_Dy) i) n → (1)

Table- defines the notations used in the equation 1

Notation	Definition
D_x	The number of partitions in x-direction
D_y	The number of partitions in y-direction
i=1	Obtain login indicators by touching the screen with hand grasped
i=2	Obtain login indicators by predefined images
n	The number of pass-images set by user

5. Login / Register

After performing the random guess attack we get to know that this application will provide a secure user-id / password based secured login mechanism to access its services.

6. Upload Image

This is the main module in this application. The Main Process in the Mex application will be worked here. The bill picture is already stored in the mobile gallery .the user will select the picture from the gallery and upload it to the server. And also upload the details like employee name, employee id and Bill details. All the details uploaded here is stored in the wamp server

7. View Status

After uploading the details the user can check the status of the request using the same application. The status will be shown as pending until the higher authority accepts or cancels the Request

8. View Request

The User Requested data can be viewed by the higher authority. Admin is the authority to accept or reject the request. This module is done by using PHP. The Admin will use System to view the request.

9. Approve / Cancel After viewing the Request the admin can have the permission to accept or reject the request. The user can check the status.

ALGORITHMS IMPLEMENTED

Random Guess Attack

Step 1: The attacker randomly tries each square as a possible pass-square for each pass image until a successful login occurs.

Step 2: The key security determinants of the system are the number of pass-images and the degree of discretization of each image.

Step 3: To quantify the security of Pass Matrix against random guess attacks, we define the entropy of a password space as in equation given below,

Entropy = log2 ((Dx_Dy) i) n

Step 4: If the entropy of a password space is k bits, there will be 2kpossible passwords in that space.

PassMatrix

Step 1: Passmatrix will consist of images in the square matrix.

Step 2: The user will choose the desired pass-squares to secure his / her system of devices in the passmatrix system.

Step 3: Sequence number of images will be decided according to the user's demand.

CONCLUSION

With the increasing trend of web services and apps, users are able to access these applications anytime and anywhere with various devices. 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 easily be cracked through shoulder surfing. Using traditional textual passwords or PIN method, users need to type their passwords to authenticate themselves and thus these passwords can easily be revealed 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. Pass Matrix is a novel and easy-to-use graphical password authentication system, which can effectively alleviate shoulder-surfing attacks. In addition, Pass Matrix can be applied to any authentication scenario and device with simple input and output capabilities.

REFERENCES

[1] S. Sood, A. Sarje, and K. Singh, “Cryptanalysis of passwordauthentication schemes: Current Status and Key Issues,” in Methodsand Models in Computer Science, 2009. ICM2CS 2009.Proceeding ofInternational Conference on, Dec 2009, pp. . 1–7.

[2] S. Gurav, L. Gawade, P. Rane, and N. Khochare, “Graphicalpassword authentication: Cloud securing scheme,” in ElectronicSystems, Signal Processing and Computing Technologies (ICESC), 2014International Conference on, Jan 2014, pp. 479–483.

[3] K. Gilhooly, “Biometrics: Getting Back to Business,” Computerworld, May, vol. 9, 2005.

[4] R. Dhamija and A. Perrig, “Deja vu: A User Study Using Imagesfor Authentication,” in Proceedings of the 9th Conference on USENIXSecurity Symposium-Volume 9. USENIX Association, 2000, pp. 9-13. 4–4.

[5] “Realuser,” http://www.realuser.com/.

[6] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, “Thedesign and Analysis of Graphical Passwords,” in Proceedings of the 8th Conference on USENIX Security Symposium-Volume 8. USENIXAssociation, 1999, pp. 1–1.

[7] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, “Passpoints: Design and longitudinal evaluation of a graphicalpassword system,” International Journal of Human-Computer Studies, Vol. 63, no. 1-2, pp. 102-127, 2005.