A Shoulder Surfing Resistant Graphical Authentication System

Sowduri Thejovathi[1], Dr. G V Ramesh Babu[2]
M.C.A, M.Tech, Ph.D

***Abstract*- Authentication based on passwords is used largely in applications for computer security and privacy. 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. 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 PassMatrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, PassMatrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks. We also implemented a PassMatrix prototype on Android and carried out real user experiments to evaluate its memorability and usability. From the experimental result, the proposed system achieves better resistance to shoulder surfing attacks while maintaining usability.**

EXISTING SYSTEMS

In order to be more secure than the existing Android pattern password with entropy 18:57 bits against brute force attacks, users have to set two pass-images and use the graphical method to obtain the one-time login indicators. Like most of other graphical password authentication systems, PassMatrix is vulnerable to random guess attacks based on hot-spot analyzing. 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. According to an article in Computer world, a security team at a large company ran a network password cracker and surprisingly cracked approximately 80% of the employees' passwords within 30 seconds [3]. Textual passwords are often insecure due to the difficulty of maintaining strong ones.

DRAWBACK

Textual passwords are vulnerable to eves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as alternative techniques to textual passwords. Most of the graphical schemes are vulnerable to shoulder surfing. To address this problem, text can be combined with
images or colors to generate session passwords for authentication.

PROPOSED SYSTEMS

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 PassMatrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, PassMatrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks. a lot of research on password authentication has been done in the literature. Among all of these proposed schemes, this paper focuses mainly on the graphical-based authentication systems. To keep this paper concise, we will give a brief review of the most

related schemes that were mentioned in the previous section. The accuracy perspective focuses on the successful login rates in both sessions, including the practice logins. The usability perspective is measured by the amount of time users spent in each PassMatrix phase.

Advantage:

Two techniques are proposed to generate session passwords using text and colors which are resistant to shoulder surfing. The habitual movements and the preference of users that the attacker may take advantage of to figure out the potential passwords.

1) Any communication between the client device and the server is protected by SSL so that packets or information will not be eavesdropped or intercepted by attackers during transmission.
2) The server and the client devices in our authentication system are trustworthy.
3) The keyboard and the entire screen of mobile devices are difficult to protect, but a small area (around 1:5 cm2) is easy to be protected from malicious people who might shoulder surf passwords.
4) Users are able to register an account in a place that is safe from observers with bad intention or surveillance cameras that are not under proper management.

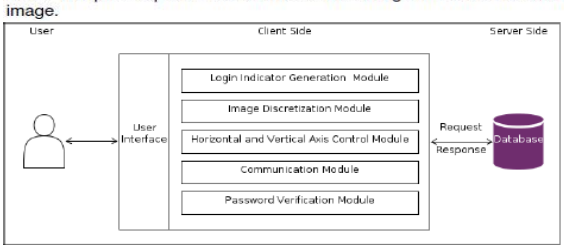
MODULE DESCRIPTION

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 (1) the security weakness of the traditional PIN method, (2) the easiness of obtaining passwords by observers in public, and (3) 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 n images. The number of images (i.e., n) is user-defined. Figure 5 demonstrates the proposed scheme, in which the first pass-square is located at (4, 8) in the first image, the second pass-square is on the top of the smoke in the second image at (7, 2), and the last pass-square is at (7, 10) in the third image. In Pass Matrix, users choose one square per image for a sequence of n images rather than n squares in one image as that in the Pass Points [7] scheme. 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 on an incorrect region within the image the login will be failed

Fig. 5. A password contains three images (n=3) with a pass square in each. The pass squares are shown as 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 the select the image that he can to log in, this will the provide more security.

. 11. (a) The Main page of PassMatrix, users can register an accou
ıctice or start to log in for experiment. (b) Users can choose from
of 24 images as their pass-images. (c) There are 7×11 squares
ch 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 setting according to the regions. But in this type of authentication we choose the color coordinates for 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 space as in equation 3. Table 7 defines the notations used in the equation. If the entropy of a password space is k bits, there will be 2kpossible passwords in that space.

5. Login / Register

MeX 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 in to the server. And also upload the details like employee name , employee id and Bill details. All the details uploaded here is stored in to 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 accept or cancel the Request

8. View Request

The User Requested data can be view 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

SOFTWARE REQUIREMENTS:

Operating System	: Windows
Technology	: Java and J2EE
Web Technologies	: Html, JavaScript, CSS
IDE	: My Eclipse
Web Server	: Tomcat
Network	: LAN
Database	: My SQL
Java Version	: J2SDK1.5

HARDWARE REQUIREMENTS

Hardware	:	Pentium
Speed	:	1.1 GHz
RAM	:	1GB
Hard Disk	:	20 GB
Floppy Drive	:	1.44 MB
Key Board	:	Standard Windows Keyboard
Mouse	:	Two or Three Button Mouse
Monitor	:	SVGA

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 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. Because of the design of the horizontal and vertical bars that cover the entire pass-image, it offers no clue for attackers to narrow down the password space even if they have more than one login records of that account. Furthermore, we implemented a Pass Matrix prototype on Android and carried out user experiments to evaluate the memorability and usability. The experimental result showed that users can log into the system with an average of 1:64 tries (Median=1), and the Total Accuracy of all login trials is 93:33% even two weeks after registration. The total time consumed to log into Pass Matrix with an average of 3:2 pass-images is between 31:31 and 37:11 seconds and is considered acceptable by 83:33% of participants in our user study.

Based on the experimental results and survey data, 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. The survey data in the user study also showed that Pass Matrix is practical in the real world.

Mex Application is one of the useful application in the current situation. This is the easy way to communicate with the admin. Employee expense claim workflow became an early candidate for enablement as it could eliminate handling of supporting expense bills and instead use the camera of Smartphone to capture the bill