Shoulder Surfing Resistant Graphical Authentication System

M.Kannadasan, J.Amarnadha reddy, K.Venkata Raman

Abstract— 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.

Index Terms— Introduction , existing system,proposed system,module description,algothim implemented,system specification, conclusion

1.Introduction

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. 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 proved 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 regarded as the weakest link in the authentication chain . Therefore, a n authentication scheme should be designed to overcome these vulnerabilities. In this paper, we present a secure graphical authentication system named PassMatrix that 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.

2.EXISTING SYSTEM

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.

.

3.PROPOSED SYSTEM

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 proved 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 regarded as the weakest link in the authentication chain [16]. Therefore, an authentication scheme should be designed to overcome these vulnerabilities. In this paper, we present a secure graphical authentication system named PassMatrix that protects users from becoming victims of shoulder surfing attacks when inputting passwords in public through the usage of one-time

- *M.Kannadasan is currently pursuing Master of Computer Applications in KMM Institute of PG studies in S.V University, Andhra pradesh, PH-7097310302. E-mail: kannadasanmkds@gmail.com*
- *J.Amarnadha reddy is currently pursuing Master of Computer Applications in KMM Institute of PG studies in S.V University, Andhra pradesh, PH-8500069351. E-mail: amarnadhareddy143@gmail.com.*
- *K.Venkata Ramana is currently working as principal in KMM Institute of PG studies in S.V University, Andhra pradesh, PH-9866742584.*

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.

4.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

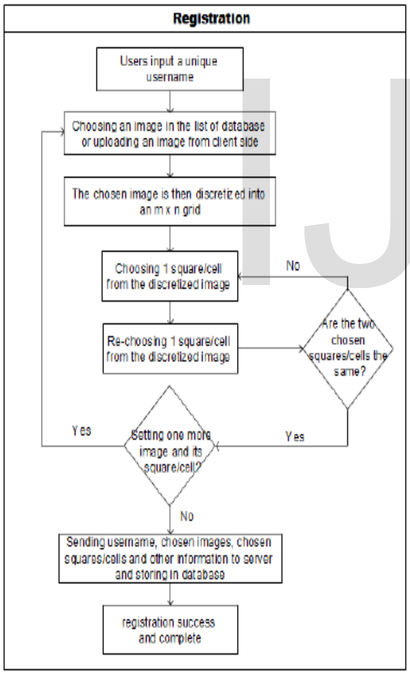

Registration
Users input a unique username
Choosing an image in the list of database or uploading an image from client side
The chosen image is then discretized into an m x n grid
Choosing 1 square/cell from the discretized image
No
Re-choosing 1 square/cell from the discretized image
Are the two chosen squares/cells the same?
Yes
Setting one more image and its square/cell?
Yes
No
Sending username, chosen images, chosen squares/cells and other information to server and storing in database
registration success and complete

Fig. 9. The flowchart of registration phase in PassMatrix.

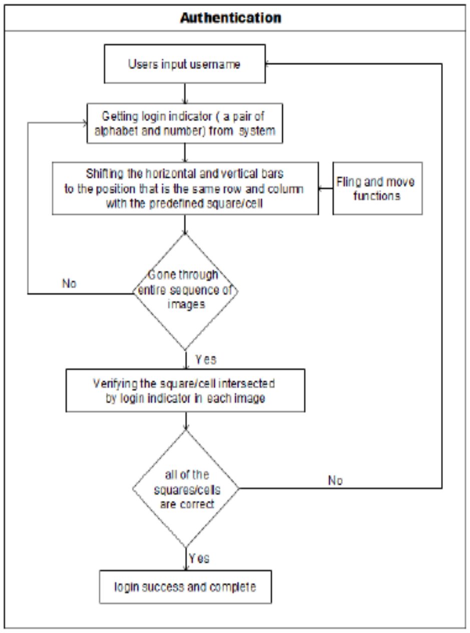

Authentication
Users input username
Getting login indicator (a pair of alphabet and number) from system
Shifting the horizontal and vertical bars to the position that is the same row and column with the predefined square/cell
Fling and move functions
No
Gone through entire sequence of images
Yes
Verifying the square/cell intersected by login indicator in each image
all of the squares/cells are correct
No
Yes
login success and complete

Fig. 10. The flowchart of authentication phase in PassMatrix.

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 PassMatrix. In PassMatrix, 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. Bellow figure demonstrates the proposed scheme, in which the first pass-square is located at in the first image, the second pass-square is on the top of the smoke in the second mage at , and the last pass-square is at in the third image. In PassMatrix, 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 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

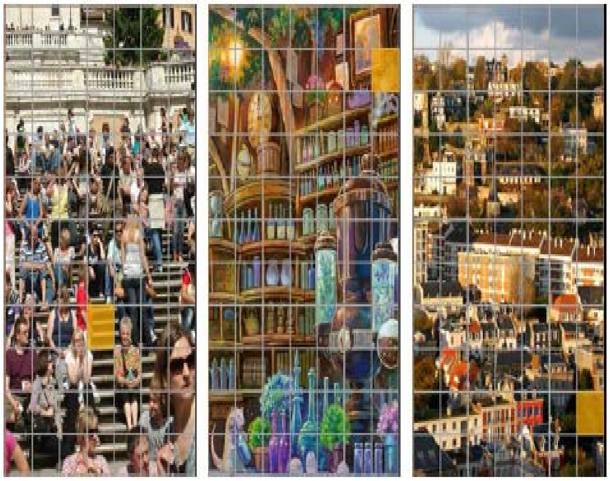
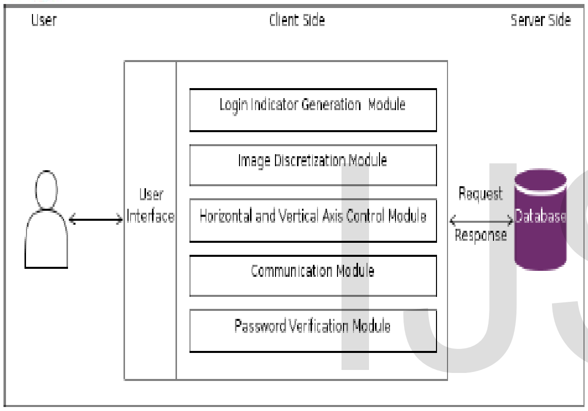


Fig. 5. A password contains three images (n=3) with a pass square in each. The pass squares are shown as the orange-filled area in each image.


User
Client Side
Server Side
Login Indicator Generation Module
Image Discretization Module
User Interface
Horizontal and Vertical Axis Control Module
Communication Module
Password Verification Module
Request
Response
Database

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.

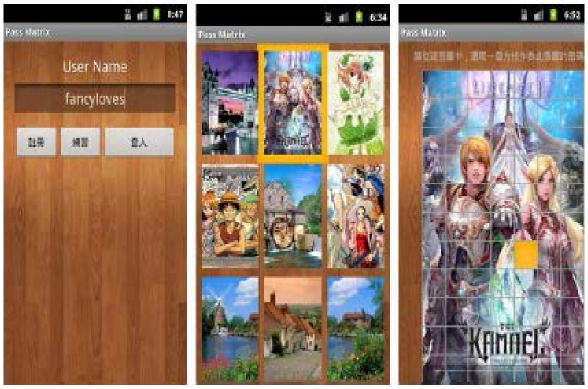


Fig. 11. (a) The Main page of PassMatrix, users can register an account, practice or start to log in for experiment. (b) Users can choose from a list of 24 images as their pass-images. (c) There are 7 × 11 squares in each image, from which users choose one as the pass-square.

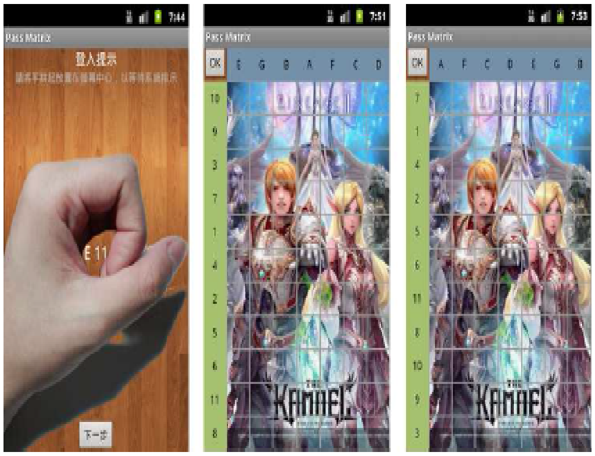


Fig. 12. (a) A visual way for users to obtain a one-time valid login indicator. (b) The permutations of alphanumerics in horizontal and vertical bars are randomly generated for each image. (c) Users can shift the bars to the correct position so that the login indicator aligns with the pass-square.

Color Image Authentication

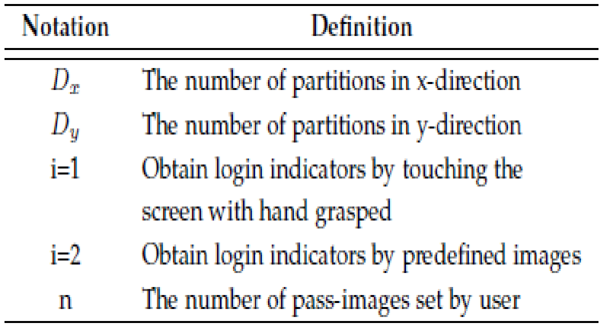
In this type the authentication is user by the color coordinates of that position. In normal Authentication the password is setting according to the regions. But in this type of authentication we choose the color coordinates for password setting

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 PassMatrix against random guess attacks, we define the entropy of a password space as in equation3. 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.

Entropy = log2((Dx_ Dy)i)n

TABLE 7
The definition of notations used in equation 3.



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

Login / Register

The application will provide a secure user-id/password based secured login mechanism to access its services.

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 tomcat server

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

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

Approve / Cancel

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

5.ALGOTHIM IMPLEMENTED

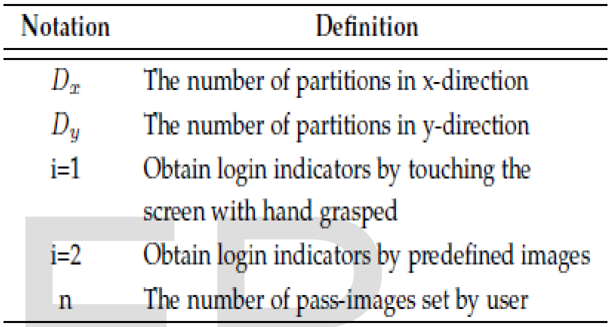
Random Guess Attack

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 PassMatrix against random guess attacks, we define the entropy of a password space as in equation3. 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.

Entropy = log2((Dx_ Dy)i)n

TABLE 7
The definition of notations used in equation 3.



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

6.SYSTEM SPECIFICATION

Hardware Requirements:

- System : Pentium IV 3.5 GHz or Latest Version.
- Hard Disk : 40 GB.
- Monitor : 14’ Colour Monitor.
- Mouse : Optical Mouse.
- Ram : 1 GB.

Software Requirements:

- Operating system : Windows XP or Windows 7, Windows 8.
- Coding Language : Java / J2EE (Jsp,Servlet)
- Data Base : My Sql Server
- Documentation : MS Office
- IDE : Eclipse Galileo
- Development Kit : JDK 1.6
- Server : Tomcat 6.0

7. CONCLUSION:

With the increasing trend of web services and apps, users are able to access these applications anytime and any where 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 between31:31 and 37:11 seconds and is considered acceptable by83:33% 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.

The 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

REFERENCES:

[1] S. Sood, A. Sarje, and K. Singh, "Cryptanalysis 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. Gurav, L. Gawade, P. Rane, and N. Khochare, "Graphical password authentication: Cloud securing scheme," in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International 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 images for authentication," in Proceedings of the 9th conference on USENIX
Security Symposium-Volume 9. USENIX Association, 2000, pp. 4-4.

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

[6] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The
design and analysis of graphical passwords," in Proceedings of the 8th conference on USENIX Security Symposium-Volume 8. USENIX Association, 1999, pp. 1-1.

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

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

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

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