ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

Implementation of Graphical Authentication System for Shoulder Surfing Attacks

Keerthana M.M[1], Archana MR[2]

Assistant Professor, Dept. of CSE., ATME College of Engineering, Mysuru , Karnataka , India[1]

Assistant Professor, Dept. of CSE., ATME College of Engineering, Mysuru , Karnataka , India[2]

ABSTRACTAuthentication 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 '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 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, pass matrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks. We also implemented a pass matrix 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.

KEYWORDS: Shoulder surfing attacks, Pass matrix

I. 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. Even worse, it is not a rare case that users may use only one username and password for multiple accounts. 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 employee's passwords within 30 seconds. Textual passwords are often insecure due to the difficulty of maintaining strong ones. 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. However, most of these image-based passwords are vulnerable to shoulder surfing attacks (SSAs). This type of attack either uses direct observation, such as watching over someone's shoulder or applies video capturing techniques to get passwords, PINs, or other sensitive personal information. 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, an authentication scheme should be designed to overcome these vulnerabilities. In this paper, we present a secure graphical authentication system named Pass Matrix 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

DOI: 10.15680/IJIRCCE.2018.0602069

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

II. RELATED WORK

[1] An Association –Based Graphical Password Design Resistant to Shoulder-Surfing Attack

Author presents 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, we further improve our primary design to overcome the shoulder-surfing attack issue without adding any extra complexity into the authentication procedure. System performance analysis and comparisons are presented to support our proposals.

[2] Pass - thoughts: Authenticating with our minds

Author presents a novel idea for user authentication that we call pass-thoughts. Recent advances in Brain Computer Interface (BCI) technology indicate that there is potential for a new type of human-computer interaction: a user transmitting thoughts directly to a computer. The goal of a pass-thought system would be to extract as much entropy as possible from a user’s brain signals upon “transmitting” a thought. Provided that these brain signals can be recorded and processed in an accurate and repeatable way, a pass-thought system might provide a quasi two-factor, changeable, authentication method resilient to shoulder-surfing. The potential size of the space of a pass-thought system would seem to be unbounded in theory, due to the lack of bounds on what composes a thought, although in practice it will be finite due to system constraints. In this paper, author discusses the motivation and potential of pass thought authentication, the status quo of BCI technology.

[3] A User Study Using Images for Authentication

Current secure systems suffer because they neglect the importance of human factors in security. Author addresses 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. Author examines therequirements of a recognition-based authentication system and proposes 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] The design and analysis of graphical passwords.

In this paper author propose and evaluate new graphical password schemes that exploit features of graphical input displays to achieve better security than text-based passwords. Graphical input devices enable the user to decouple the position of inputs from the temporal order in which those inputs occur, and we show that this decoupling can be used to generate password schemes with substantially larger (memorable) password spaces. In order to evaluate the security of one of our schemes, we devise a novel way to capture a subset of the "memorable" passwords that, we believe, is itself a contribution.

III. PROPOSED METHODOLOGY

3.1 Existing System

In the Existing System Users actions such as typing from their keyboard or clicking on the pass-images or pass-points in public may reveal their passwords to people with bad intention. Existing System is vulnerable to shoulder surfing attacks.Every time you use an ATM to transaction with your bank, you are vulnerable to a certain kind of theft known as SHOULDER SURFING. That is when someone waits for you to enter your personal identification number and swoops in to withdraw cash before you are fully logged out of the systemShoulder surfing is the practice of spying on the user of a cash dispensing machine or other electronic device in order to obtain their personal identification number, password, etc. This has become the larger problem now days.

Disadvantages of the Existing System

- Existing System is vulnerable to shoulder surfing attacks.
- Type-I: Naked eyes.
- Type-II: Video captures the entire authentication process only once.
- Type-III: Video captures the entire authentication process more than once.

3.2 Proposed System

To overcome

- The security weakness of the traditional PIN method.
- The easiness of obtaining passwords by observers in public.
- The compatibility issues to devices.

In the Fig 3 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. 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 point's scheme.

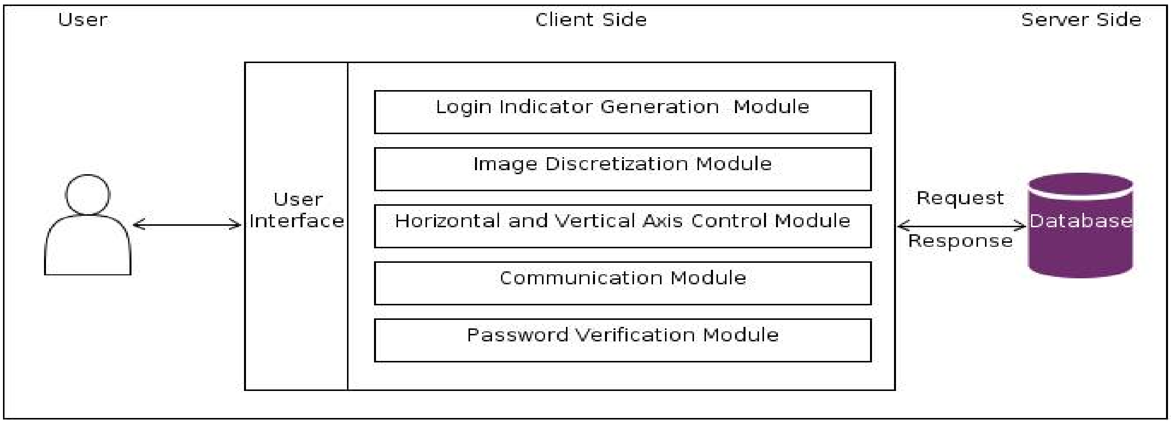

User
Client Side
Server Side
User Interface
Login Indicator Generation Module
Image Discretization Module
Horizontal and Vertical Axis Control Module
Communication Module
Password Verification Module
Request
Response
Database

Fig 1: Overview of proposed system

- **Login Indicator Generator Module**

This module generates a login indicator consisting of several distinguishable characters or visual materials for users during the authentication phase. In our implementation, we used characters A to F and 1 to 8 for a 6 × 8 grid. Both letters and numbers are generatedrandomly and therefore a different login indicator will be provided each time the module is called.

- **Image Discretization Module**

This module divides each image into squares, from which users would choose one as the pass-square. An image is divided into a 6× 8 grid. The smaller the image is discretised, the larger the password space is.

- **Horizontal and Vertical Axis Control Module**

There are two scroll bars: a horizontal bar with a sequence of letters and a vertical bar with a sequence of numbers. This control module provides drag and fling functions for users to control both bars. Users can fling either bar using their finger to shift one alphanumeric at a time. They can also shift several checks at a time by dragging the bar for a distance.

- **Communication Module**

This module is in charge of all the information transmitted between the client devices and the authentication server.

- **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 login indicator to a pass-square will be described in the next section.

- **Database**

The database server contains several tables that store user accounts, passwords (ID numbers of pass images and the positions of pass-squares), and the time duration each user spent on both registration phase and login phase. Pass Matrix has all the required privileges to perform operations like insert, modify, delete and search.

3.2.1 Advantages of the Proposed System

- Proposed system is invulnerable to all types of Shoulder Surfing Attacks such as,
  Type-I: Naked eyes.
  Type-II: Video captures the entire authentication process only once.
  Type-III: Video captures the entire authentication process more than once.
- It overcomes the security weakness of the traditional PIN method.
- It overcomes the easiness of obtaining passwords by observers in public.

3.3 Feasibility Study

Feasibility is the determination of whether or not a project is worth doing. The process followed in making this determination is called feasibility Study. This type of study if a project can and should be taken. In the conduct of the feasibility study, the analyst will usually consider seven distinct, but inter-related types of feasibility.

3.3.1 Technical Feasibility

This is considered with specifying equipment and software that will successful satisfy the user requirement the technical needs of the system may vary considerably but might include

- The facility to produce outputs in a given time.
- Response time under certain conditions.
- Ability to process a certain column of transaction at a particular speed.

3.3.2 Economical Feasibility

Economic analysis is the most frequently used technique for evaluating the effectiveness of a proposed system. More commonly known as cost / benefit analysis. The procedure is to determine the benefits and savings are expected form a proposed system and a compare them with costs. It benefits outweigh costs; a decision is taken to design and implement the system will have to be made if it is to have a chance of being approved. There is an ongoing effort that improves in accuracy at each phase of the system life cycle.

3.3.3 Operational Feasibility

It is mainly related to human organization and political aspects.

- What changes will be brought with the system?
- What organizational structures are distributed?
- What new skills will be required?
- Do the existing system staff members have these skills?
- If not, can they be trained in the course of time

IV. SYSTEM ARCHITECUTURE

System architecture is a conceptual model that defines the structure, behavior and more views of a system; an architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviours of the system.

DOI: 10.15680/IJIRCCE.2018.0602069

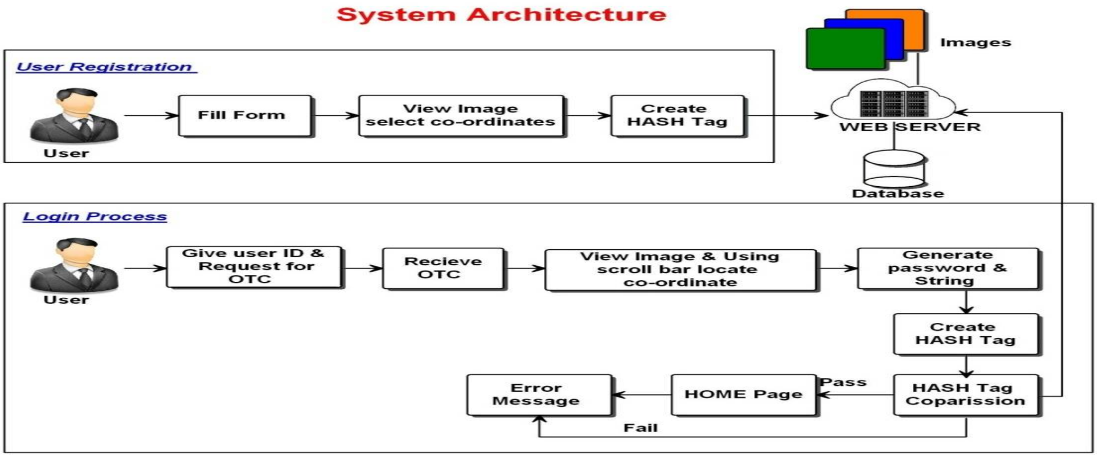


Fig 3: System Architecture for Shoulder Surfing Resistant Graphical Authentication System application

The above diagram Fig.5.2 represents the overview of Shoulder surfing resistant graphical authentication system architecture .The system architecture consist of user registration and login process as shown in the above diagram .

- **User Registration**
  - User enters complete details in form.
  - Selects the image co-ordinates.
  - Hash tags are created.
  - Everything is stored in database.
- **Login process**
  - User gives user id and request for OTP.
  - Receives OTP.
  - Generates password using hash tag.
  - Using scroll bar locates the co-ordinates.

4.1 Use case diagram of Admin

Use case diagrams are the one which describes the system and the verity of its user and represents the interactions of users with the system through different use cases. Use cases are important requirement techniques that have been widely used in modern software engineering.

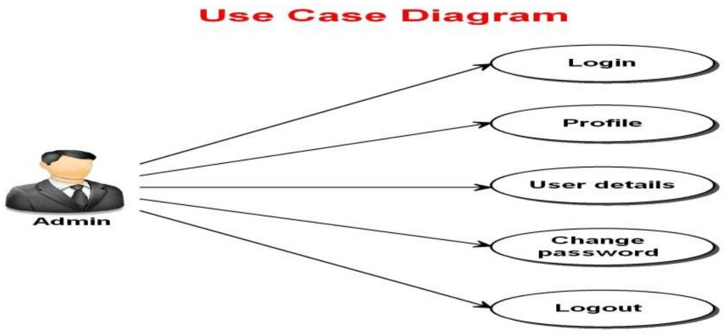


Fig 4: Use case diagram of Admin for Shoulder Surfing Resistant Graphical Authentication System application

In the above Fig.4 use case diagram of admin interacts with

- **Login:** login page for admin to authenticate.
- **Profile:** profile page display the contents of login page.
- **User details:** user details consist of the user form to get full complete details.
- **Change password:** admin have permission to change password to new password.
- **Logout:** logout option will sign-out the admin.

4.2 Use case diagram of user

New user, login, BMI, change password, logout are the user interactions with the system.

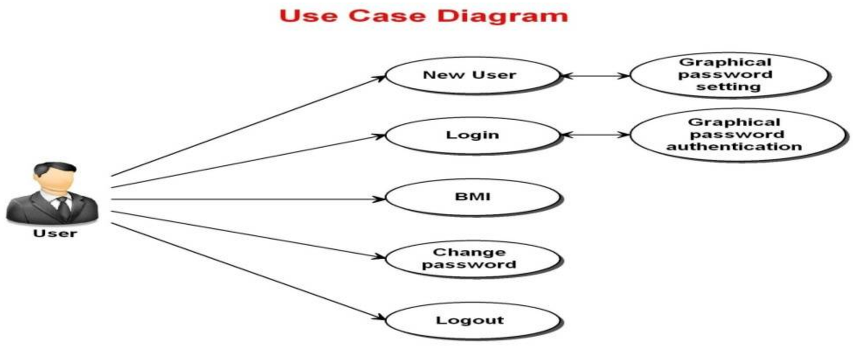
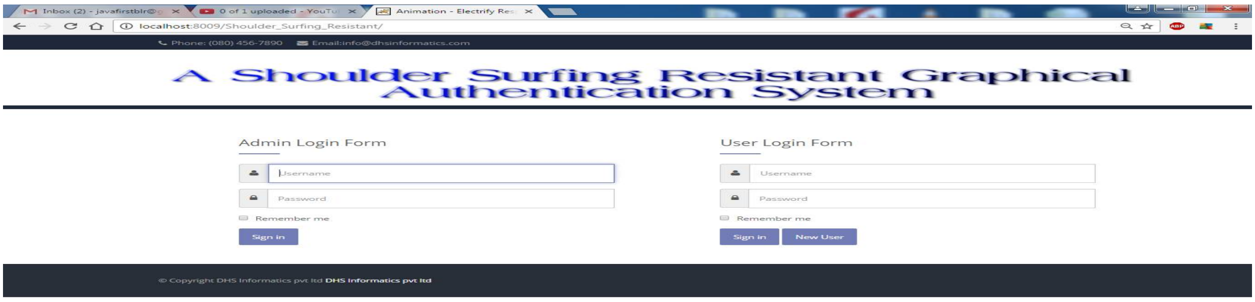


Fig 5: Use case diagram of User for Shoulder Surfing Resistant Graphical Authentication System application.

IV. EXPERIMENTAL RESULTS


Inbox (2) - javafirstblr@g
0 of 1 uploaded - YouTu
Animation - Electrify Res
localhost:8009/Shoulder_Surfing_Resistant/

Phone: (080) 456-7890 Email:info@dhsinformatics.com

A Shoulder Surfing Resistant Graphical Authentication System

Admin Login Form

Username

Password

□ Remember me

Sign in

User Login Form

Username

Password

□ Remember me

Sign in New User

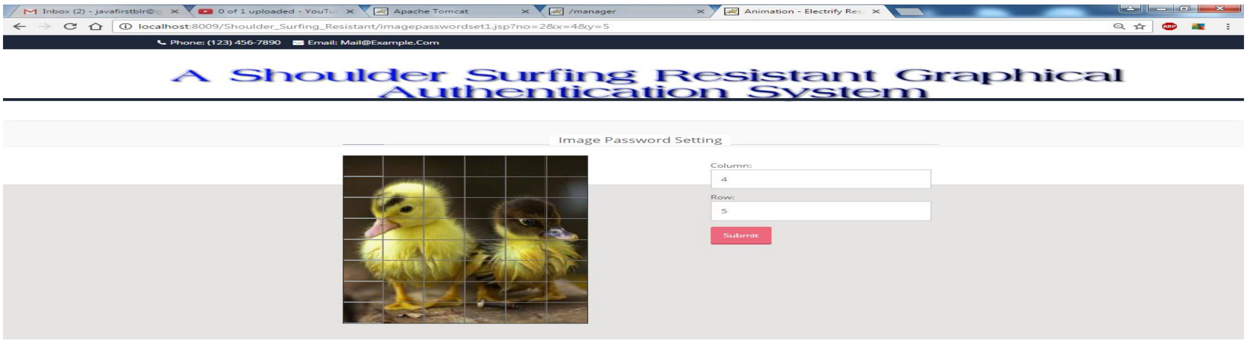
© Copyright DHS Informatics pvt ltd **DHS Informatics pvt ltd**

Fig 6: Home Page

The above Fig 6 describes that Home page consists of both admin login form and formally in the login mode. Participant should create an account consisting of username and a password.

4.3 Image Password Settings

The image password setting is done by the user in the following way, each image will be displayed on the screen, and the user will be having (6*10) squares to select in each image. After the user selects the coordinates, the corresponding column and the row will be filled with the selected coordinates and the list of coordinates will be stored in the database



localhost:8009/Shoulder_Surfing_Resistant/imagepasswordset1.jsp?no=2&x=4&y=5

Phone: (123) 456-7890 Email: Mail@Example.Com

A Shoulder Surfing Resistant Graphical Authentication System

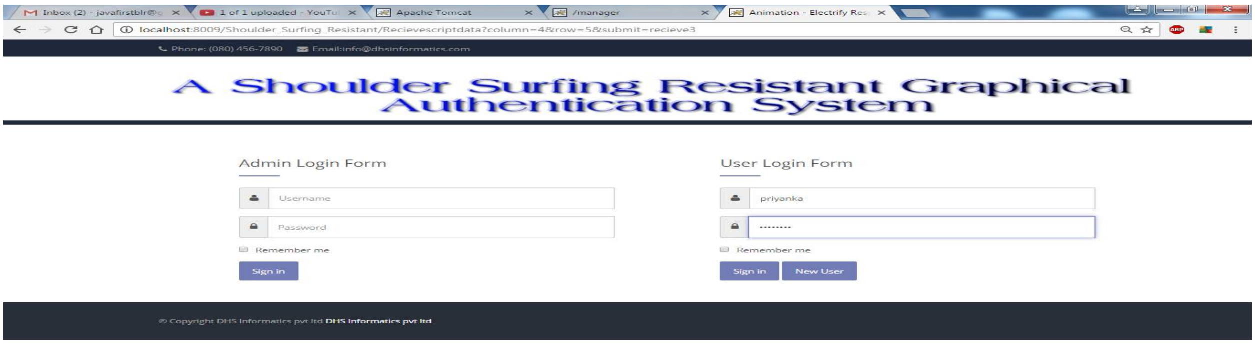
Image Password Setting

Column: 4

Row: 5

Fig 7: Password Setting For Image 1

Fig 7 shows setting up of password for image 1.



localhost:8009/Shoulder_Surfing_Resistant/Recievescriptdata?column=4&row=5&submit=recieve3

Phone: (080) 456-7890 Email:info@dhsinformatics.com

A Shoulder Surfing Resistant Graphical Authentication System

Admin Login Form

Username

Password

□ Remember me

User Login Form

priyanka

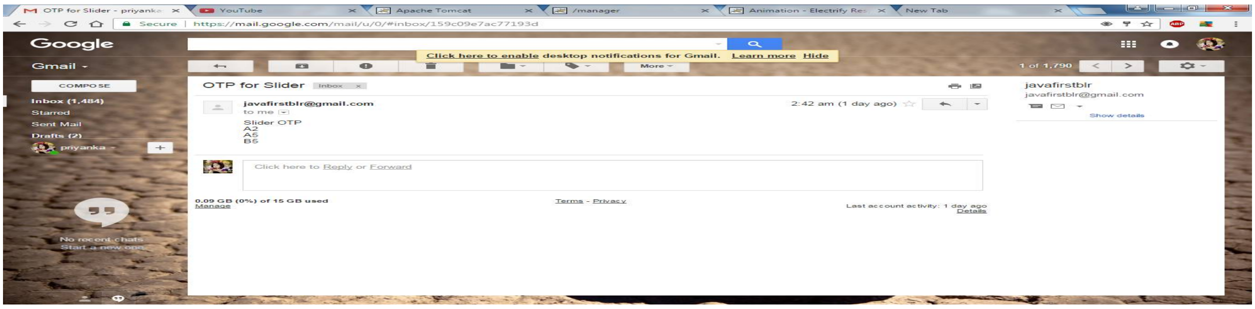
•••••••••

□ Remember me

© Copyright DHS Informatics pvt ltd DHS Informatics pvt ltd

Fig 8: User Login Process

After the completion of registration with the user details, further sign in process of the user is directly done through the user login form by entering the username and password.



Secure | https://mail.google.com/mail/u/0/#inbox/159c09e7ac77193d

Click here to enable desktop notifications for Gmail. Learn more Hide

OTP for Slider

javafirstblr@gmail.com
to me

2:42 am (1 day ago)

Slider OTP
A2
A5
B5

Click here to Reply or Forward

0.09 GB (0%) of 15 GB used
Manage

Last account activity: 1 day ago
Details

javafirstblr
javafirstblr@gmail.com

Fig 9: OTP from Mail

The first step in login phase is getting the one time valid login indicator from the system. Here letters and numbers are generated randomly and therefore a different login indicator will be provided each time the module is called.

For instance, if the user chooses the square (4, 2) then the login indicator will be (A,2).

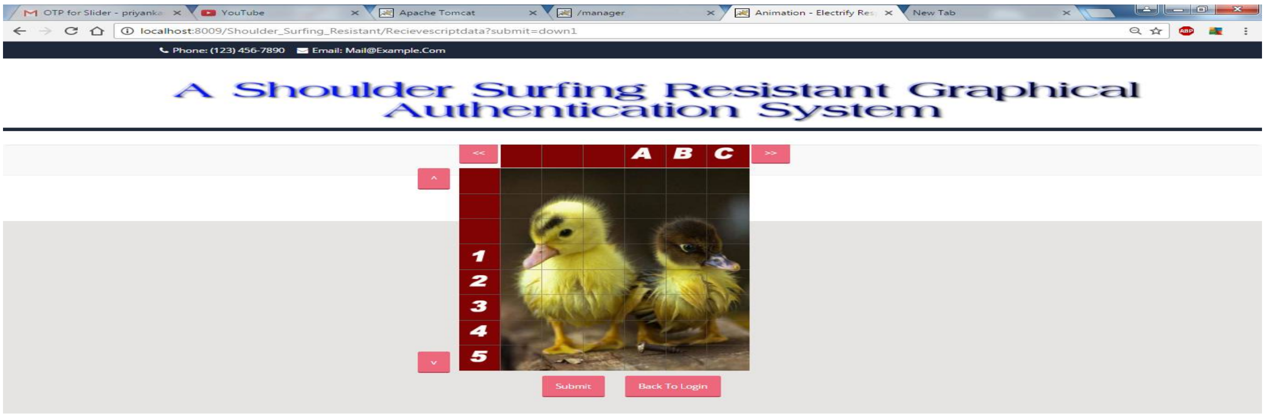

OTP for Slider - priyanka
YouTube
Apache Tomcat
/manager
Animation - Electrify Res
New Tab
localhost:8009/Shoulder_Surfing_Resistant/Recievescriptdata?submit=down1
Phone: (123) 456-7890
Email: Mail@Example.Com
A Shoulder Surfing Resistant Graphical Authentication System
<<
A
B
C
>>
^
1
2
3
4
5
v
Submit
Back To Login

Fig 10: Rearranging The Coordinates

This verifies the user passing during authentication phase. The first pass-image will be shown on the display, with a horizontal bar and a vertical bar on its top and left respectively. To respond to the challenge, the user flings or drags the bars to align the pre-selected pass-square of the image with the login indicator. For example, if the indicator is (E, 8) and the pass-square is at (4,2) in the grid of the image, the user shifts the character ”E” to the 4th column on the horizontal bar and ”8” to the 2th row on the vertical bar .

V. CONCLUSION AND FUTUREWORK

With the increasing trend of web services and apps, users are able to access these applications anytime and anywhere with various devices. 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.

A major advantage of persuasive cued click point scheme is its large password space over alphanumeric passwords. There is a growing interest for graphical passwords, although the main argument for graphical password is that people are better at memorizing graphical passwords than text-based passwords. Online password guessing attacks on password-only systems have been observed for decade’s present-day attackers targeting such systems are empowered by having control of thousand to million node botnets. In previous ATT-based login protocols, there exists a security-usability trade-off with respect to the number of free failed login attempts (i,e., with no ATT’s and other requirements). In contrast, PGRP is more restrictive against brute force and dictionary attacks while safely allowing large number of free failed attempts for legitimate users. PGRP is apparently more effective in preventing password guessing attacks; it also offers more convenient login experience, e.g., fewer ATT challenges for legitimate users. PGRP appears suitable for organizations of both small and large number of user accounts.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

REFERENCES

1. R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years,"ACMComput. Surveys, vol. 44, no. 4, 2012.
2. J. A. Halderman, B. Waters, E. W. Felten, "A Convenient Method for Securely Managing Passwords", Proc. International World Wide Web ACM Conference, pp. 471-479, May 2005.
3. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proc. 8th USENIX Security Symp., 1999, pp. 1–15.
4. H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," Int. J. Netw. Security, vol. 7, no. 2, pp. 273–292, 2008.
5. H. Gao, X. Liu, S.Wang, and R. Dai, "A new graphical password scheme against spyware by using CAPTCHA," in Proc. Symp. Usable Privacy Security, 2009, pp. 760–767.
6. Sonia Chiasson, P.C. van Oorschot, and Robert Biddle, "Graphical Password Authentication Using Cued Click Points" ESORICS, LNCS 4734, pp.359- 74, Springer- Verlag Berlin Heidelberg 2007.
7. Manu Kumar, Tal Garfinkel, Dan Boneh and Terry Winograd, "Reducing Shoulder-surfing by Using Gazebased Password Entry", Symposium On Usable Privacy and Security (SOUPS) , July 18-20, 2007, Pittsburgh,PA, USA.
8. R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of9th USENIX Security Symposium, 2000.
9. L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.
10. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.
11. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42, pp. 41-46, 1999.
12. S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in *Proceedings ofMidwes Instruction and Computing Symposium*, 2004.
13. Zhi Li, Qibin Sun, Yong Lian, and D. D. Giusto, „An association-based graphical password design resistant to shoulder surfing attack", International Conference on Multimedia and Expo (ICME), IEEE.2005.
14. S. Li, S. A. H. Shah, M. A. U. Khan, S. A. Khayam, A.-R. Sadeghi, and R. Schmitz, "Breaking e-banking CAPTCHAs," in *Proc. ACSAC*, 2010, pp. 1–10.

BIOGRAPHY

Ms. Keerthana M M is an assistant professor in Dept. of computer science and engineering in ATME College of Engineering Mysuru, Karnataka, India. She received her master degree in computer science and engineering from VKIT, Bangalore affiliated to VTU University, Belagavi. She has 3 years teaching experience and her field of interest is cloud computing.

Mrs. Archana M R is an assistant professor in Dept. of computer science and engineering in ATME College of Engineering Mysuru, Karnataka, India. She received her master degree in computer network and engineering from NIE, Mysuru . She has 11 year of teaching experience and her field of interest is image processing.