OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

SHOULDER SURFING RESISTENT GRAPHICAL AND PAIR BASED AUTHENTICATION SYSTEM

Prof. Shaikh Mudassir[1],Rohan Khaire[2]

Asst Professor[1], P.G. Student[2],Department of Computer Science & Engineering, Everest College of Engineering & Technology, Aurangabad, Maharashtra, India

----

Abstract: **The authentication based on the passwords is used mostly in applications for the computer security and privacy. However, the human actions such as selecting less secured passwords credentials and inputting passwords in an insecure way are considered "the weakest link" within the authentication chain. Instead of arbitrary alphanumeric strings, users tend to select passwords either short or purposeful for simple memorization. With internet applications and mobile apps pile up, individuals will access these applications anywhere and anytime with different devices. This evolution brings good convenience however it will increases the probability of exposing passwords credentials to shoulder surfing attacks. Attackers will observe directly or use external recording devices to get users' credentials. To overcome this issue, proposed a novel authentication system named Pass-Matrix, which is based on graphical passwords to resist shoulder surfing attacks. Implemented a Pass-Matrix prototype on web applications and allotted real user experiments to describe its memorability and usefulness. From the experimental result, is shown that, the proposed system achieves better resistance to shoulder surfing attacks whereas maintaining usability.**

KEYWORDS: Pass matrix, paired based, Image Discretization, authentication, Shoulder Surfing Attack..

---∴.∴.∴.---

I INTRODUCTION

The primary goal of improving the current user authentication technology is to make the method secure yet easier for the user. Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated particularly by the fact that humans can remember pictures better than text. Psychological studies have shown that people can remember pictures better than text [8]. Pictures are generally easier to be remembered or recognized than text, especially photos, which are even easier to be remembered than random pictures. It has also been suggested that graphical passwords may be hard to guess or broken by brute force search.

List of Problems Shoulder Surfing Attack

- The problem of shoulder surfing attacks when logging in public.
- Making password easy to remember passwords of many accounts.
- Making password more secure than traditional PIN.
- The problem of efficiently search exact password objects during the authentication phase.
- The problem of requiring users to memorize extra

information or to perform extra computation during authentication.

Scope

- The system is applicable to pc and system will be able to provide secure login for personal account.
- Limited usability of authentication schemes that can be applicable to some devices only.

Objectives

- To Secure authentication system by selection of image as password.
- To restrict the shoulder surfing by attackers.
- To increase the complexity of the login systems.
- Divide image into blocks and assigning random block number for user selected block.

II SYSTEM DEVELOPMENT

Image Discretization module:

First step is module divides each image into squares, from which users would choose one as the pass-square. Segmentation of image is perform by system.

Login Indicator generator Module:

This module generates a login indicator consisting of several distinguishable characters (such as alphabets and

numbers) or visual materials (such as colors and icons) for users during the authentication phase.

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. The bars are used to implicitly point out (or in other words, align the login indicator to) the location of the users pass-square.

Communication Module:

This module is in charge of all the information transmitted between the client devices and the authentication server. Any communication is protected by SSL (Secure Socket Layer) protocol and thus, is safe from being eaves-dropped and intercepted.

Password Verification:

This module verifies the user password during the authentication phase. A pass-square acts similar to a password digit in the text-based password sys- tem. The user is authentication 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, pass- words (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.

In this system use the java language for development. Users can register an ac- count, log in a few times in practice mode, and then log in for the experiment with a clients device. Used JAVA including username checking, pass images listing, im- age discretion, pass-squares selection, login indicator delivery, and the horizontal and vertical bars circulation. In the server side of our implementation, we MySQL to store and fetch registered accounts to/from the database to handle the password verification.

Advantage of this is to secure login system for personal use of accounts. Limited usability of authentication schemes that can be applicable to some devices only.

Requirement Gathering:

Requirement analysis is for transformation of operational need into software de-scription, software performance parameter, and software configuration through use of standard, iterative process of analysis and trade-off studies for understanding what the customer wants analyzing need, assessing feasibility, negotiating a reasonable solution validating the specification and managing the Requirements.

Purpose:

The purpose of System Requirements Analysis is to obtain a thorough and de- tailed understanding of the

business need as defined in Project Origination and cap- tured in the Business Case, and to break it down into discrete requirements, which are then clearly defined, reviewed and agreed upon with the Customer Decision-

Requirement analysis is software engineering task that bridges the gap between system level software description and design module. Requirement analysis is the important part of software life cycle. This forms the base for design and development. decides whether it should relate to other system or not.

III DESIGN AND IMPLEMENTATION CONSTRAINTS

High level design means abstract view of the system where details are not shown. High level design does contain class diagram at conceptual level and no operations are defined at high level. Low level design uses class diagram at implementation level with most of the required detail. Low Level Document (LLD) consist each class thorough description which includes method and property name and every possible details. Currently we are going to concentrate on the high level design that includes UML Diagram and Structure Diagram.
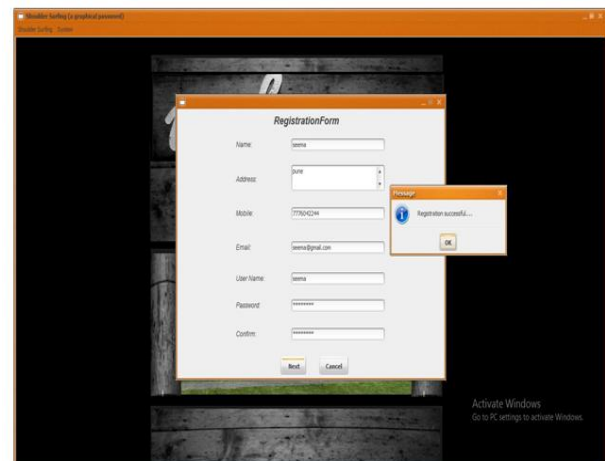

Figure 1: Registration

Figure 2: Image Upload
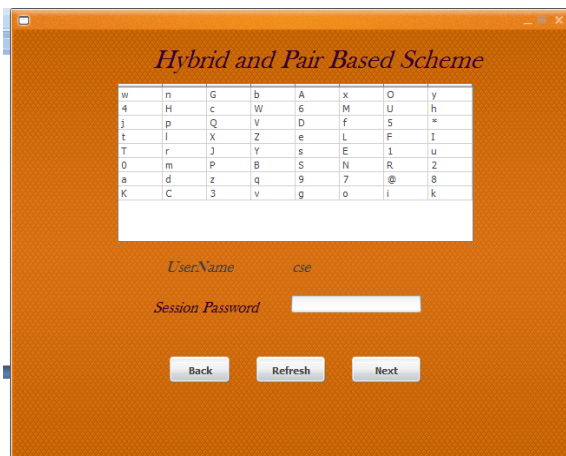
Figure 3: Pas-square selection from image Form
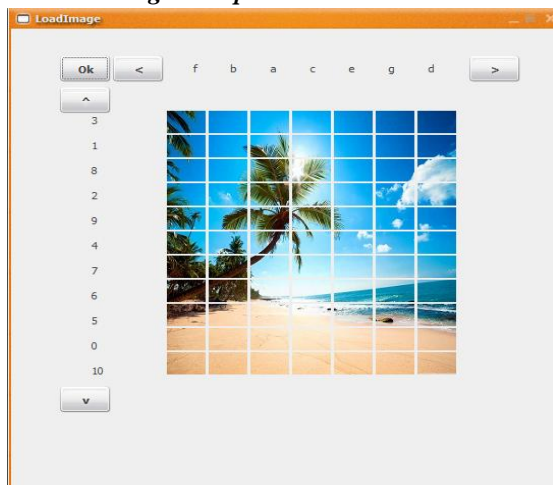

Figure 4: pair Based Scheme

Figure 5: Graphical Password Scheme

Project Quality And Testing

Testing is a process used to help identify the correctness, completeness and quality of developed computer software. Here testing activities are enlisted which have been carried out for the dissertation. It describes the software test environment for testing, identifies the tests to be performed and provides schedules for test activities.

Goals and objectives

The main goals of software testing is:

- To find out the errors during program execution.
- Refine the system by removing the errors.
- To test the software for performance degradation under stress.
- Design the system in a modular way so that application of various data values exposes the hidden bugs in the system.
- To review every module in a detailed way internally as well as at boundary level.
- To use several testing tools and schemes of black box and white box testing.
- To follow the system life cycle and help in maintaining the system.

IV CONCLUSION

We have studied different methods for graphical password authentication scheme. 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 will test our system to evaluate memorability and usability.

Future Scope

Now in proposed system image grids are constant at particular location which leads to password guessing attack, so to overcome this limitation in future images grids are varied also numbers are varied this will be difficult to guess.

REFERENCES

[1] A. C. L. Andrew S. Patrick, Scott Flinn, "HCI and Security Systems," in CHI,
Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA., 2003.
[2] A. 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.
[3] K. Gilhooly, "Biometrics: Getting Back to Business," in *Computerworld, May 09*, 2005.
[4] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in *Proceedings of 9th USENIX Security Symposium*, 2000.
[5] M. Kotadia, "Microsoft: Write down your passwords," in *ZDNet Australia, May 23*, 2005.
[6] A. Gilbert, "Phishing attacks take a new twist," in *CNET News.com, May 04*,
2005.
[7] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," *Communications of the ACM*, vol. 33, pp. 168-176, 2000.

[8] R. N. Shepard, "Recognition memory for words, sentences, and pictures," *Journal of Verbal Learning and Verbal Behavior*, vol. 6, pp. 156-163, 1967.

[9] A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real- World Security," in *Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce*, 1999.

[10] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in *Proceedings of Midwest Instruction and Computing Symposium*, 2004. 57

[11] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can'tRecall," in *Proceedings of Conference on Human Factors in Computing Systems (CHI)*. Vienna, Austria: ACM, 2004, pp. 1399-1402.

[12] L. Sobrado and J.-C. Birget, "Graphical passwords," *The Rutgers Scholar, AnElectronic Bulletin for Undergraduate Research*, vol. 4, 2002.

[13] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in *Proceedings of International conference on security and management*. Las Vergas, NV, 2004.

[14] S. Man, D. Hong, and M. Mathews, "A shoulder-surfing resistant graphicalpassword scheme," in *Proceedings of International conference on security and management*. Las Vegas, NV, 2003.