Multi Way Authentication With Image And Auto Dialing Options For Secured Bank Transactions

Rekha.G [1], Dr V. Saravanan[2]
Department of Information Technology
[1] PG Student, Hindusthan College of Arts and Science, Coimbatore, India
[2] HOD & Professor, Hindusthan College of Arts and Science, Coimbatore, India

Abstract- *Authentication is the process to establish the identity of a communication partner. It is an essential security component of today's many Internet applications. The security weaknesses of using text based passwords for user authentication are well known but most systems still rely heavily on this simple and low cost solution. There is a significant body of recent research exploring the feasibility of alternative approaches to provide a more secure and usable authentication solution. One promising alternative is graphical passwords. Based on studies showing that human brain is better at recalling images than text, these unconventional methods aim to solve memory burden and low entropy problems of classical passwords.*

Click based graphical passwords that use background images suffer from hotspot problem. Previous graphical password schemes based on recognition of images do not have a sufficiently large password space suited for most Internet applications. In this project, a novel graphical password method is proposed based on recognition of images to solve the hotspot problem. In click-based graphical password schemes, users click a sequence of points on a pictorial background to create and use passwords.

If user forgets the click area or wrongly enter password for more than 3 attempts, then the login will be temporarily blocked. User can retrieve OTP to mobile based on request, through that user can login and do transactions.

I. INTRODUCTION

Authentication is the process to establish the identity of a communication partner. It is an essential security component of today's many Internet applications. The security weaknesses of using text based passwords for user authentication are well known but most systems still rely heavily on this simple and low cost solution. There is a significant body of recent research exploring the feasibility of alternative approaches to provide a more secure and usable authentication solution. One promising alternative is graphical passwords. Based on studies showing that human brain is better at recalling images than text, these unconventional methods aim to solve memory burden and low entropy problems of classical passwords.

Click based graphical passwords that use background images suffer from hotspot problem. Previous graphical password schemes based on recognition of images do not have a sufficiently large password space suited for most Internet applications. In this paper, a novel graphical password method is proposed based on recognition of images to solve the hotspot problem. In click-based graphical password schemes, users click a sequence of points on a pictorial background to create and use passwords.

II. SYSTEM ANALYSIS

EXISTING SYSTEM

In the existing system the billing alone is maintained in FoxPro. The card details, the deposit details, the withdrawal details, the account balance details are maintained manually. The study of the existing system revealed that the system has several drawbacks. Users separately apply for account and waiting for apply ATM and net banking until receiving account number. User spend more time in bank to apply and transfer amount

Existing graphical password scheme allows user to select either the full image or various hotspots in the same image. To browse the web through mobile separate website will be created.

DISADVANTAGES

- Default click points in the image
- N number of images
- Time consumption for creating separate web site

PROPOSED SYSTEM

The proposed system is been developed to maintain and to enhance the Banking Process. the administrators to maintain the card details, the deposit details, the withdrawal

details, the account balance details. User can apply for Bank account, TM, and for net banking. After getting customer id and pin, user can access the net banking. Using net banking User can book tickets, recharge mobile phones and transfer to another account. And also secure proceeds with hidden camera.

Proposed graphical password scheme allows user to select particular area on an image for a sequence of images. Along with this content adaptation scheme was proposed for mobile web browsing.

ADVANTAGES

- User preferred hotspots
- Limited number of images
- No time consumption for creating separate website

III. MODULE DESCRIPTION

The modules identified in this project are:

- Bank Admin Module
- Login And Mail Autodialing
- Customer Module
- Cued click points
- Discretization method

Bank Admin Module

Bank admin checks the user's registration form details and creates new account for the users .it contains users personal details like phone number, address, photo, account details like account number, tm card details the pin number and account number will be sent to user's mail ID. Bank Admin can view the user's account details For reference and maintains user's account details.

Login And Mail Autodialing

In this Project user should enter their Id and password to enter into their account. If someone enters wrong password or User ID, it allows trying for three times to enter into their account after that it blocks the user Id and Capture the image of that customer or user and Send E-Mail Alert then make a call to the Corresponding user's Mobile and Administrator's Mobile.

Customer Module:

The user login to his account using OTP and color Password Authentication and do operations transaction, cash withdraw, cash deposit Get Receipt etc.

Cued Click Points

In Cued Click Points (CCP), users select a particular area on each of c = 2 images rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point.

In this user selects their own preferred area on each of the images rather than more hotspots on one image. It makes attacks based on hotspot analysis and offer cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click point.

Discretization Method

User cannot be able to remember the exact Cued Click Points in an image. To avoid the difficulty in remembering the exact Cued Click Points, discretization method was introduced. A discretization method is used to determine a click-point's tolerance square and corresponding grid. For each click-point in a subsequent login attempt, this grid is retrieved and used to determine whether the click-point falls within tolerance of the original point.

IV. SYSTEM IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus, it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

Figure 1. Registration form

The implementation stage involves careful planning, investigation of the existing system and its constraints on

implementation, designing of methods to achieve changeover and evaluation of changeover methods.

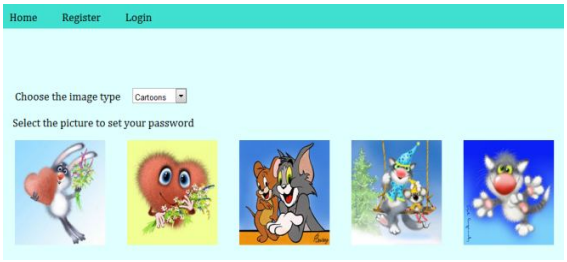

Figure 2. Image Selection

The project is implemented by accessing simultaneously from more than one system and more than one window in one system. The application is implemented in the asp.net under the Windows 7 Professional and accessed from various clients.

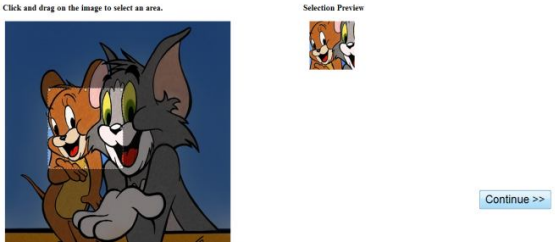

Figure 3. Image Copy area Selection Page

V. CONCLUSION & FUTURE ENHANCEMENT

.

Authentication process has been successfully designed, tested and implemented in a systematic manner. Graphical password provides high authentication for user accounts and the web pages can be easily adapted for the requested website by using content adaptor. The user of the system easily understands how to access and control the system. It is also found that the project reduces the time consumption for creating web site and increases the complexity for attackers.

The project was developed using ASP .NET, it can be future enhance to AJAX, WEB 2.0 for website development. Currently the web parsing is implemented for a single website, by using various algorithms all the websites can be adapted. The security of CCP also deserves closer examination, and should address how attackers might exploit the emergence of hotspots

REFERENCES

[1] D. Chaum, "Untraceable electronic mail return addresses and digital pseudonyms", Communications of the ACM, 1981.

[2] L. Breslau, P. Cao, L. Fan, G. Phillips, S. Shenker, "Web caching and Zipf-like distributions: evidence and implications", Proceedings of IEEE INFOCOM, 1999.

[3] D. Goldschlag, M. Reed, P. Syverson, "Onion routing", Communications of the ACM, 1999.

[4] M. K. Reiter, A. D. Rubin, "Crowds: anonymity for web transactions", ACM Transactions on Information and System Security, 1998.

[5] S. Saroiu, P. Gummadi, S. Gribble, "A measurement study of Peer-to-Peer file sharing systems", Proceedings of Multimedia Computing and Networking, 2002.

[6] K. Sripanidkulchai, "The popularity of Gnutella queries and its implications on scalability", Proceedings of The O'Reilly Peer-to-Peer and Web Services Conference, 2001.

[7] V. Scarlata, B. N. Levine, C. Shields, "Responder anonymity and anonymous Peer-to-Peer file sharing", Proceedings of IEEE ICNP, 2001.

[8] I. Abraham, D. Malkhi, "Probabilistic quorums for dynamic systems", Proceedings of DISC, 2003.

[9] R. Sherwood, B. Bhattacharjee, A. Srinivasan, " P 5 : A protocol for scalable anonymous communication ", Proceedings of IEEE Symposium on Security and Privacy, 2002.

[10] S. Sen, J. Wang, "Analyzing Peer-to-Peer traffic across large networks", Proceedings of ACM SIGCOMM Internet Measurement Workshop, 2002.