Multimedia Based Authentication System - Restraint to Shoulder Surfing

G.Sravanthi [#1], Harmeeth kaur S[#2], Prof.T.Venkat Narayana Rao [#3]

[#] *Department of Computer Science and Engineering*
Guru Nanak Institutions Technical Campus,
Rangareddy, Andhrapradesh,

[1]g.sravanthi5792@gmail.com
[2]harmeethkaur07@gmail.com
[3]tvnrbobby@yahoo.com

Abstract—**Traditionally, alphanumeric passwords have been used for user authentication. Since the passwords should be easily remembered and the passwords are to be random enough it is very difficult to create passwords satisfying both the conditions. As a result, users have the tendency to create short and simple passwords or write it in a file and store it in an insecure place. To resolve this difficulty researchers have suggested multimedia passwords. Since humans are supposed to remember pictures and sound better than random alphanumeric passwords, multimedia based passwords are supposed to be remembered and recalled easily. But shoulder surfing is one of the main problems of these passwords. So a user friendly multimedia password with resistance to shoulder surfing is a good authentication system. In this system, we propose that the user would be selecting fake passwords based on pattern to login rather than using the correct password image or sound chosen by him/her at the time of registration. Usability testing of the system showed that users were able to enter their multimedia password accurately and they can remember the passwords over a period of time. This facility would be a reality in the future, where in passwords are becoming vital aspects of security domain.**

Keywords— **Authentication system, Multimedia passwords, Shoulder surfing, Password security, Password usability**

I. INTRODUCTION

Information and computer security is supported largely by passwords which are the principle part of the authentication process. The most widespread computer authentication method is to use alphanumerical username and password which has significant drawbacks. To overcome the vulnerabilities of traditional methods, multimedia password schemes have been developed as possible alternative solutions to text-based scheme[3][4].

This system deals with the ideology which is multimedia based authentication that contains pictures and sounds which are used as passwords. Major idea of the system proposed in this paper is to create an authentication system that is secure and not vulnerable to shoulder surfing, hidden camera and spyware attacks. We have efficiently implemented the multimedia based authentication system which includes easier passwords to memorize and use. The Traditional text-based password scheme, which is used by majority of security systems, consists of user id as claim of identity and a password that supports the claim. Since the passwords have to be random enough and they have to easily remembered and users tend to compromise on the security. Users either create same password, use it for multiple systems, or they tend make a note of the passwords in a file or some use other unsecure method to remember the passwords. This is going to defeat the very purpose of an authentication system. Later graphical password scheme was developed in which the user would select images as their passwords .This system did not excel as the security measure in this system was extremely low and was vulnerable to shoulder surfing attacks.

The three insights, in combinations, comprise the essential basis of our proposed password scheme.

- Users are able to remember multimedia elements such as a picture or a sound well.
- With today's technology, it is not heavy to add multimedia passwords scheme to the text-based password scheme which has been built in computer systems.
- Mathematically we can achieve the following: we ask a user to choose k icons as a part of his password. Then we arbitrarily position $N >> k$ icons, including the k chosen ones (as a part of their password), on a screen. Then positions of k pass objects, we will surely have two and only three different cases each of which happens with the probability 1/3.Since the k pass objects are the part of password the user will understand what is happening and can respond correctly. In the mean time ,since the k pass objects are hidden in the N objects it is hard for the shoulder surfing attacker to make correct response, and more difficult to obtain the password.

II. BACKGROUND AND NEED FOR MULTIMEDIA BASED AUTHENTICATION SYSTEMS –RESTRAINT TO SHOULDER SURFING

A. *What is the need for Multimedia Based Authentication System – Restraint to Shoulder Surfing?*

The most common user authentication method is the text-based password scheme that a user enters a login name and a password. These negative points of this method have been familiar. Users usually tend to single out short passwords or passwords that are easy to remember[1] , which makes the passwords vulnerable for attackers to break. To resist brute force search and dictionary attacks, users need to use and pick long and random passwords. Unfortunately, such passwords are hard to remember. Additionally, textual password is vulnerable to shoulder-surfing, hidden-camera and spyware attacks. Graphical password schemes have been projected as a possible alternative to text-based schemes, motivated moderately by the fact that humans can remember pictures better than text [8]. In addition, the possible password space of a graphical password scheme may exceed that of text based schemes and thus presumably offer higher intensity of security. Hence, it is a additional difficulty to devise automated attacks for graphical passwords[2] . Hence we observe that, the graphical password schemes provide a way of making more human-friendly passwords while increasing the level of security. Outstanding to these advantages, there is increasing attention in graphical password. On the other hand, existing graphical passwords are far from perfect. Characteristically, system requirements and communication costs for graphical passwords are significantly higher than text-based passwords. Over that, few graphical systems support keyboard inputs. More significantly, most of the contemporary and prevailing graphical passwords are more vulnerable to shoulder-surfing attacks than textual passwords.

B T*he Existing Systems and their Vulnerabilities*

A solution to security issues that became evident as the first multi-user operating systems were being developed. There are many designated graphical password scheme's in which a password is created by having the user click on several locations on an image. During authentication, a user must click on the approximate areas of those locations. The image is used to support users to recall their passwords and therefore this method is considered more convenient than textual passwords. The "Pass Point" system extended Blonder's idea by eliminating the predefined boundaries and allowing arbitrary images to be used [8]. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to generate a password. Easiness in the order of each chosen pixel is calculated. To authenticate, the user must click within the tolerance of the chosen pixels. "Pass face" is a technique brought into usage by Real User Corporation based on the assumption that people can recall human faces easier than other pictures[5]. The basic idea is as follows. The user is asked to choose four images of human faces from a face database as their future password. In the authentication stage, the user is presented with a grid of nine faces, with many of the one face previously chosen by the user and eight decoy faces. The user has to recognize and click anywhere on the known face. This procedure is repeated for numerous rounds. The user is then done and is authenticated if he/she correctly identifies all the faces. Jermyn, et al. [6]. In that proposed technique, called "Draw a Secret (DAS)", which allows the user to draw their unique password. When creating password, a user is asked to draw simple picture on a 2D grid. The coordinates of the grids unavailable by the picture are stored in the order of the drawing. Throughout the process of authentication, the user is asked to re sketch the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated. Jermyn suggested that given reasonable-length passwords in a 5 ∗ 5 grid, the full password space of DAS is larger than that of the full text password space. Some further research based on DAS was conducted [7]. There is a common weakness in the above graphical password schemes: they are all vulnerable to shoulder surfing attacks. To deal with this issue, Sobrado and Birget developed a graphical password technique. In their scheme, the system first displays a number of 3 pass-objects (pre-selected by a user) among many other objects. To be genuine, a user needs to recognize pass-objects and click inside the triangle formed by the 3 pass-objects . Similarly , other shoulder-surfing resistant algorithm was also proposed in which a user selects a number of pictures as pass-objects. Each pass-object has several variants each variant is assigned a unique code. During authentication, the user is confronting with several scenes. Each one the scenes contains several pass-objects and many decoy-objects. Here the user needs to type in a string with the unique codes corresponding to the pass-object variants present in the scene as well as a code indicating the relative location of the pass objects in reference to a pair of eyes. Hong, et al. later this comprehensive approach to allow the user to assign their own codes to pass-object variants[4]. However, these methods force the user to memorize too many text strings, and the basic shoulder-surfing resistant property is not strong either. Table I depicts various method evolved so far along with their methodologies and probable drawback properties.

TABLE I .

Methodology	Drawbacks
Signal processing and translation algorithms-extract as much entropy as possible from a user's brain signals[6]	Not accurate and repeatable recording and processing of brain signals, requirement for a new hardware component and the associated performance
Game-like graphical method of authentication that extends the challenge response paradigm	Longer time to carry out the authentication
User enters sensitive input by selecting from an on-screen keyboard using only the orientation of their pupils	Similar error rates to those of using a keyboard and needs marginal additional time over using it
Using shapes of strokes on the grid as the origin passwords, changing the login interface of the system	Method is relativity unfamiliar to the general people, longer login process and more secure than registration phase

III. Proposed System and SYSTEM Perspective

The authentication system designed in this report is a multimedia-based password authentication system stopping shoulder surfing and also making it more user friendly than the triangle scheme or movable frame method. When the user first registers, the user has to select 5 images of 100 images shown to him. The images shown him will have some themes like cartoons, animals, flowers etc. The sounds contain basic sounds of bells, horns or some widespread ringtones etc.So that it would be easy for the user to remember. During the registration the user would create a username. The user must also provide an email id to which the communication emails (registration email/password reset email) will be sent. Every single one of the images/sounds selected by user will be saved in the database along with the user id's message digest generated using SHA1 (Secure Hash Algorithm 1) and the email id. The message digest is being generated using MessageDigest class of Java Cryptographic Extension. Before registering the user, the user id's message digest will be checked in the data base. If the message digest exists then the user will be asked to select another user id. In case if someone hacks into the database, there is no possibility for the hacker to get any user ids from the data base.

Registered users will get an email from the system explaining the process to login. The email will have the below content on the basis of the type of password chosen as password (image/sound).

Your registration is successful.

Login process:

1. Enter your user id

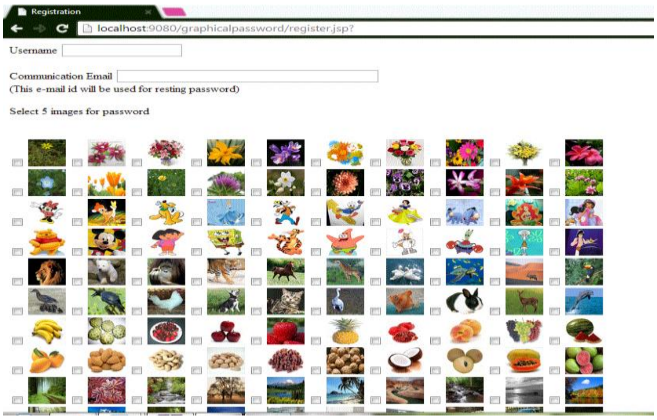
(If you have chosen picture as your password).

2. Two out of five your chosen password (images) will be displayed as part of 30 (5x6 table) images. Select the image that is situated below your chosen password. In case your chosen password is in last row of the table, select the image from the same column in top most row of the table.

3. Repeat step 2 for two more times to get a successful login (If you have chosen sound as your password).

4. Two out of five your chosen password (sound) will be displayed as a part of 30 (5x6 table) sounds. Select the sound which you have chosen as password.

5. Repeat step 4 for two more times to get a successful login.



Username

Communication Email
(This e-mail id will be used for resting password)

Select 5 images for password

Fig .1Password Selection screen of the system

In cases where the password is wrong, still the user is taken through all three rounds of authentication. This also stops the shoulder surfer, if he tries to log in, then he would not be sure where exactly was he has gone wrong.

In case the user forgets his/her password, the reset email will be sent to the user communication given at the registration time, which will contain a random number and reset link. The random number is generated using the SecureRandom class of Java Cryptography Extensions. The user can only reset password if both the user id and the random number sent to him/her matches with the one in the database. The email would indicate like this:

"Please go to http://localhost:8080/multimediapassword/checkUser.jsp and reset your password using the key: 7470085683974593015".

So by doing this we are trying to provide a user friendly multimedia-based password implementation of the system is in Java, JSP and Mysql database. The system can be deployed on a tomcat web server. MVC architecture is being implemented. JSP acts as the View, Servlet as Controller and Beans (interacting with data base) act as Model as shown in figure 2.

The shoulder surfer can look at the screen, but as the passwords that are being selected are not the correct ones, unless the shoulder surfer has access to the login process for a long time, it would be difficult for him/her to repeat the process. Also the images are loaded randomly on the screen, so the position of the images won't be the same for each load of the page. Finding the position of the image would also be easy for the user than the convex hull, as he need not imagine a hull on the screen.

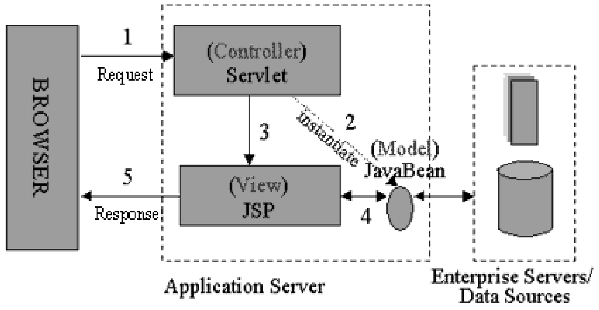


Fig. 2 MVC Architecture

IV. TEST CASES AND ANALYSIS

In this paper the multimedia based authentication system we have carried out different test cases with a wide variety of users to find out any evidential functioning flaws within the system and to test the usability in the user's point of view. We have considered each possible test cases for the testing as shown in Table II.

Each one of the below mentioned test cases have been carried out with real care and accuracy so as to find reliable results and evidential proof's.

Registration of 2 users with same user id

-In this test case we have considered taking two different users registering with the same user id and finding out the results.

Resetting the password

-Resetting password was found out much lesser compared to the other authentication systems as it is easier to remember proposed multimedia based authentication systems. However reset password option that has been used by certain users was found to be very low in number.

Login after resetting the password

-Logging in after resetting password was considered in this test case to find out the results.

Registering multiple users

-Registering multiple users was considered in this test case where each user was to obtain a new user id with a multimedia based password as a part of the process of testing.

Check for email after registration

\-Email check after the registration was used as a part of the login process to prove that the successful running of the system.

Checking database for the message digest rather than the user id

- In this test case we have checked the database for the message digest which stores several components such as user id, email address for communication and their selected passwords. Here, the message digest was preferred to be checked as a part of the testing.

TABLE II Test Cases and Result

Test Case Name	No. Of People considered for each test case	Results
Registration of 2 users with same user id	02	Successful
Resetting the password	10	Successful
Login after resetting the password	05	Successful
Registering multiple users Check for email after registration	15	Successful
Checking database for the message digest rather than the user id	20	Successful
Usability test of the system	50	Successful

V. CONCLUSION

There have been a lot of alphanumeric password based authentication systems. Since the process of creating passwords is ought to be complex at the same time easy to remember, these are the two concern points that contradict the alphanumeric password and hence researchers have suggested graphical passwords. The multimedia based passwords are a step ahead over the existing graphical password based authentication systems and they also provide a secure platform for the users as it restraint to shoulder surfing environment.

This paper presents the major functionalities and working of the Multimedia Based Authentication system restraint to shoulder surfing and this system of password security would be the most popular mechanism in the days to come.

REFERENCES

[1].Wiedenbeck S, Waters J, Sobrado L and Birget J C, "Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme" , AMC, Pages: 177 - 184, Year of Publication: 2006, ISBN:1-59593-353-0

[2]. G. Blonder, Graphical passwords, United States patent, 5559961, 1996.

[3]. Dhamija R. and Perrig, A. Déjà Vu: User study using images for authentication. In Ninth Usenix Security Symposium, 2000.

[4]. Ziran Zheng, Xiyu Liu, Lizi Yin, Zhaocheng Liu, 2009, 'A Stroke- Based Textual Password Authentication Scheme', First International Workshop on Education Technology and Computer Science (ETCS).

[5]. Manu Kumar, Tal Garfinkel, Dan Boneh, Terry Winograd, 2007, 'Reducing shoulder-surfing by using gaze-based password entry',Proceedings of the 3rd symposium on Usable privacy and security, ACM.

[6]. Julie Thrope, P. C. van Oorschot, Anil Somayaji, 2005, 'Passthoughts: authenticating with our minds', Proceedings of the 2005 workshop on New security paradigms, ACM

[7]. Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, Jean-Camille Birget, 2006, 'Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme',Proceedings of Advanced Visual Interfaces (AVI2006).

[8]. Huanyu Zhao and Xiaolin Li, 2007, 'S3PAS: A Scalable Shoulder- Surfing Resistant Textual-Graphical Password Authentication Scheme', 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW).

Authors Biographies

#1. G.Sravanthi is currently in her 4th year at the Guru Nanak Institutions Technical Campus pursuing Bachelors in Computer Science and Engineering. Over the past four years she has been actively participating in several technical presentations, seminars & workshops. She avers Computer research oriented study and has been working on computer music research. Her major interest of research lies in the areas of Computer and Network Security, Computer music, Music Composition & Orchestration, Machine learning and Image processing. She can be reached at g.sravanthi5792@gmail.com.

#2. Harmeeth kaur.s is currently in her 4th year at the Guru Nanak Institutions Technical Campus pursuing Bachelors in Computer Science and Engineering. She has been enthusiastically participating in a number of technical presentations, seminars & workshops. She has been keen on Computer research oriented study and has been working on her major interest of research in the areas of Computer and Network Security, Cognitive Computing. She can be reached at harmeethkaur07@gmail.com

#3. Professor T.Venkat Narayana Rao, received B.E in Computer Technology and Engineering from Nagpur University, Nagpur, India, M.B.A (Systems), holds a M.Tech in Computer Science from Jawaharlal Nehru Technological University, Hyderabad, A.P., India and a Research Scholar in JNTU. He has 21 years of vast experience in Computer Science and Engineering areas pertaining to academics and industry related I.T issues. He is presently working as Professor, Department of Computer Science and Engineering, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, R.R.Dist., A.P, INDIA. He is nominated as Editor and Reviewer to 28 International journals, has published 52 papers relating to Computer Science and Information Technology, and has authored many papers. He is currently working on research areas that include Image Processing, Digital Watermarking, Data Mining, Network Security and other Emerging areas of Information Technology. He can be reached at tvnrbobby@yahoo.com