INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Graphical User Authentication Using Transformation (Rotation and Resizing)

Vinay Kadyan[1] Sukhvir Singh[2]

[1]Research Scholar
[1]NCCE,
Israna, Pin no.132107
[1]vinaykadyanncce@gmail.com

[2] Associate Professor
[2]NCCE,
Israna, Pin no.132107
[2]boora_s@yahoo.com

Abstract: *User Authentication is one of the most important elements in the field of data security. It is well known that there are basically two pillar son which Graphical User Authentication is build around:Usablity and Security Text Based Password Authentication (TBPA) has several problems. In this paper we are discussing an algorithm which covers both the aspect of GUA It is now beyond any doubt that USER AUTHENTICATION is the most critical element in the field of Information Security. Text Based Password Authentication (TBPA) has shown some difficulties. Unfortunately none of the existing algorithms are able to cover both of these aspects at the same time The main purpose of this thesis is an algorithm that combines the usability & security features by Rotating and Resizing the Images.*

Keywords: *Graphical User Authentication, Graphical password, multifactor graphical authentication, Usability Features in graphical password, Security Features in graphical password, Texture, Strong Password.*

1. INTRODUCTION

Undoubtedly, there is currently the phenomenon of threats at the threshold of the internet, internal networks and secure environments.
The principle area of attack is AUTHENTICATION, which is of course the process of determining the accessibility of a user to a particular resource or system.
Generally, authentication methods are classified into three categories:

a. Inherit Based Authentication
b. Token Based Authentication
c. Knowledge Based Authentication

With the enormous number of users utilising the facilities of the internet today, authentication is fundamental for every secure system. Traditional text-based passwords have well known weaknesses.
According to these problems of text-based passwords, many new knowledge-based user authentication techniques have emerged that in theory produce higher entropy user authentication where in Graphical Authentication is one of the most important of them[1].

From the first graphical user authentication which was proposed by Blonder until now, many researchers have worked in order to propose new algorithms [4], or improve the previous ones with the intention of increasing the security and usability.
But unfortunately increasing usability for the users has caused the algorithms to have fewer security features or when the researchers focus on the security they lose the usability features.
The primary objective of this research is to design a new Graphical User Authentication namely GUABRR algorithm (Graphical User Authentication Based on Rotation and Resizing)[3].

2. LITERATURE REVIEW

The term "Picture Superiority Effect" coined by researchers to describe Graphical-Based Passwords (GBP) reflects the effect of GBP's as a solution to conventional password techniques.
Initially, the concept of Graphical User Authentication (GUA) described by Blonder (Greg, 1996), one image would appear on the screen whereupon the user would click on a few chosen regions of the image.
Most of articles from 1994 till 2009 describe that Graphical Authentication Techniques are categorised into three groups:

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

1. Pure Recall Based Techniques:
   Users reproduce their passwords, without having the chance to use the reminder marks of system. Although easy and convenient, it appears that users do not quite remember their passwords.

2. Cued Recall Based Techniques:
   Here, the system provides a framework of reminders, hints and gestures for the users to reproduce their passwords or make a reproduction that would be much more accurate.

3. Recognition Based Techniques:
   Here, users select pictures, icons or symbols from a bank of images. During the authentication process, the users have to recognise their registration choice from a grid of image[2]. Research has shown that "90% of users can remember their password after one or two months" (Saranga and Dugald 2008).

The International Organisation for Standardisation defines different models for usability. Each of algorithms discussed above lack a number of the features in these models.

(i) ISO 9241
(ii) ISO 9126
(iii) ISO 13407

3. SECURITY EVALUATION METHODS

There are two methods of security evaluation in GUA algorithms. The initial part defines the "Graphical Password Space". Then the second part defines the "Graphical Password Entropy".

***Graphical Password Space*:**
Users can pick any element for their password in GUA; the raw size of password space is an upper bound on the information content of the distribution that users choose in practice. It is not possible to define a formula for password space but for all algorithms [7] it is possible to calculate the password space or the number of passwords that can be generated by the algorithm. Now, this section will define and calculate the password space for previous algorithms and GUABRR, then make a comparative analysis.

For example, in textual passwords with length of 6 characters that can select the capital and small characters, the password space will be:

Space = 6^52

In the Pass face algorithm with **N** rounds and **M** pictures in each round, the password space will be:

Space = M^N

In the Blonder algorithm and Pass logics with **N** number of pixels on the image and **M** number of locations to be clicked, the password space will be:

Space = N^M

In the Syukri algorithm with unlimited patterns for drawing, the password space will be infinity.
In the GUABRR algorithm which includes 25 images in the images matrix, 3 to 5 images can be selected for the password, 3 characters for each password
(Alphabetic 26, numbers 10, special characters 30), and the password space will be:

Space (Based on 3 images) = (25^3) * (66^3)
Space (Based on 5 images) = (25^5) * (66^5)

Graphical Password Entropy:
Password entropy is usually used to measure the security of a generated password, which conceptually means how hard to blindly guess out the password.
For simplicity, assume all passwords are evenly distributed, the password entropy of a graphic password can then be calculated as follows.

Entropy = **N** log2 (|**L**||**O**||**C**|)

In other words, Graphical password entropy tries to measure the probability that the attacker obtains the correct password based on random guessing.
In the above formula, N is the length or number of runs, L is locus alphabet as the set of all loci, O is an object alphabet and C is colour of the alphabet. For example in a point click GUA algorithm that runs for four rounds and has 30 salient points with 4 objects and 4 colours then:

Entropy = 4 * Log2 (30*4*4) = 35.6

In an image selection algorithm with 5 runs and in each run selects 1 from 9 images then:

Entropy = 5 * Log2 (9) = 15.8

For the proposed algorithm, 3 to 5 images will be selected as passwords from 25 images, each image can rotate at 12 different degrees and resizes in 2 different sizes. So the entropy will be:

Entropy (based on 3 images) = 3 * Log2 (25*12*2)
= 27.7
Entropy (based on 5 images) = 5 * Log2 (25*12*2)
= 46.3

4. NEW PROPOSED SYSTEM

The usability and security final features that will be implemented in the proposed new GUA system prototype are shown in Table:

Vol. 1, Issue VII, Aug 2013
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

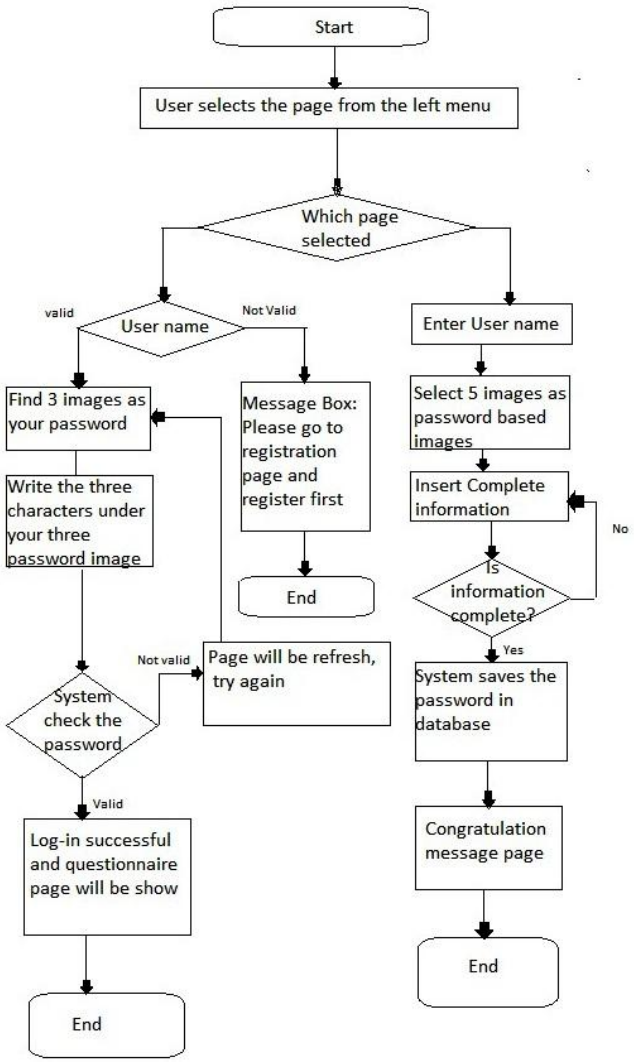
Table1: Prototypes

Usability / Security Features	Attributes	Attributes Especially for Graphical User Authentication	Abbreviation
Usability (Effectiveness)	Reliability & Accuracy	Reliability & Accuracy	R&A
Usability (Efficiency)	The utilisation in real world	Applicable	Applicable
Usability (Satisfaction)	Easy to use	Use the mouse easily	Mouse usage
	Easy to create	Select simple way to create the password	Create Simply
	Easy to memorise	Meaningful	Meaningful
		User assign image	Assignable Image
		Freedom of choice	
	Easy to execute	Select simple steps of registration and login	Simple Steps
	Good view	Select good interface	Nice interface
	Easy to understand	Simple training session	Training simply
	Pleasant	Pleasant picture	Pleasant picture
Security	Resistant on Attacks	Password Spaces, Password Entropy	-

***Framework of Proposed System*:**
The main idea of the project is that in the log-in phase, password images will appear differently from what is shown to the user during the registration phase. These images have a special process to create this deferential which is rotation and resizing of images [5]. As the size of database is one of the major weaknesses in GUA algorithms, new proposed systems only save the original images in the database. The processing like random rotation and resizing of images and random text creating of each image are generated by the proposed system during run time [6]. So, the processed images does not save in the database which cause the total size of the database to be small but the processing on the system will be high.

GUABRR Structure Overview:
The GUABRR system has two tier architecture, a client layer and a server layer. Client layer provides pages and interface for servicing the user like registration and log-in pages via a web browser such as Internet Explorer. The Client layer awaits acknowledgement from server. The server layer provides the necessary services for client side such as authentication service and user information retrieval.

Figure 1: FLOWCHART



The Server layer is handled based on forwards all requests to the server layer and the Microsoft Internet Information Server (IIS) and .net framework. Requests and acknowledgements are handled by the server which transacts with a database manager.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

5. CONCLUSIONS AND FUTURE WORK

Balancing Usability and Security will always be an issue in GUA. There are new challenges to overcome faults in authentication systems. On the other hand, advances are being made to overcome such issues. This thesis introduces a new GUA algorithm for recognition base graphical password based on Rotation and Resizing process on images as recall based algorithms.

The usability and security features extracted from this study were used to build a new algorithm called GUABRR to make the algorithm more usable and secure.

5.1 Suggestions for Future work

The current project showed simple processing on image like Rotation and Resizing create the giant step for making the algorithm more secure. This research found many other ways for making the GUA algorithms more secure and usable such as:

(i) Running "Image Processing" on the Images of GUA, for example working on color and texture histograms

(ii) Working on colored images (such as natural , human, and animals pictures)

(iii) Finding other image processing method like changing the color or changing the brightness's of pictures to increase security

REFERENCES

[1] "The Pass Points graphical password scheme", Symposium on Usable Privacy and Security 2007. Pittsburgh, Pennsylvania, USA, ACM.

[2] Alain Abran, Witold Suryn, Adel Khelifi, Juergen Rilling, Ahmed Seffah; 2003,"Consolidating the ISO Usability Models"; Concordia University, Montreal, Canada.

[3] Ali Mohamed Eljetlawi; 2008, "Study and Develop a New Graphical Password System", University Technology Malaysia, Master Dissertation.

[4] Ali Mohamed Eljetlawi, Norafida Ithnin; 2008, "Graphical Password: Comprehensive study of the usability features of the recognition base Graphica lPassword methods", Third 2008 International. Conference on Convergence and hybrid Information Technology, IEEE.

[5] Beilei Huang, Edmund M-K. Lai, A.P.Vinod, 2008," Image Resizing and Rotation Based on the Consistent Resampling Theory", 2008 International Symposiumon Intelligent Signal Processing and Communication Systems(ISPACS2008), Bangkok ,Thailand

[6] Christopher Varenhorst; 2004,"Passdoodles: a Lightweight Authentication Method ", Massachusetts Institute of Technology, Research Science Institute.

[7] "Common Attack Pattern Enumeration and Classification (CAPEC) Standard Abstraction Attack Pattern List (Release 1.3)";http://capec.mitre.org/data/lists/patabs_standard.html, Access on October 2009.