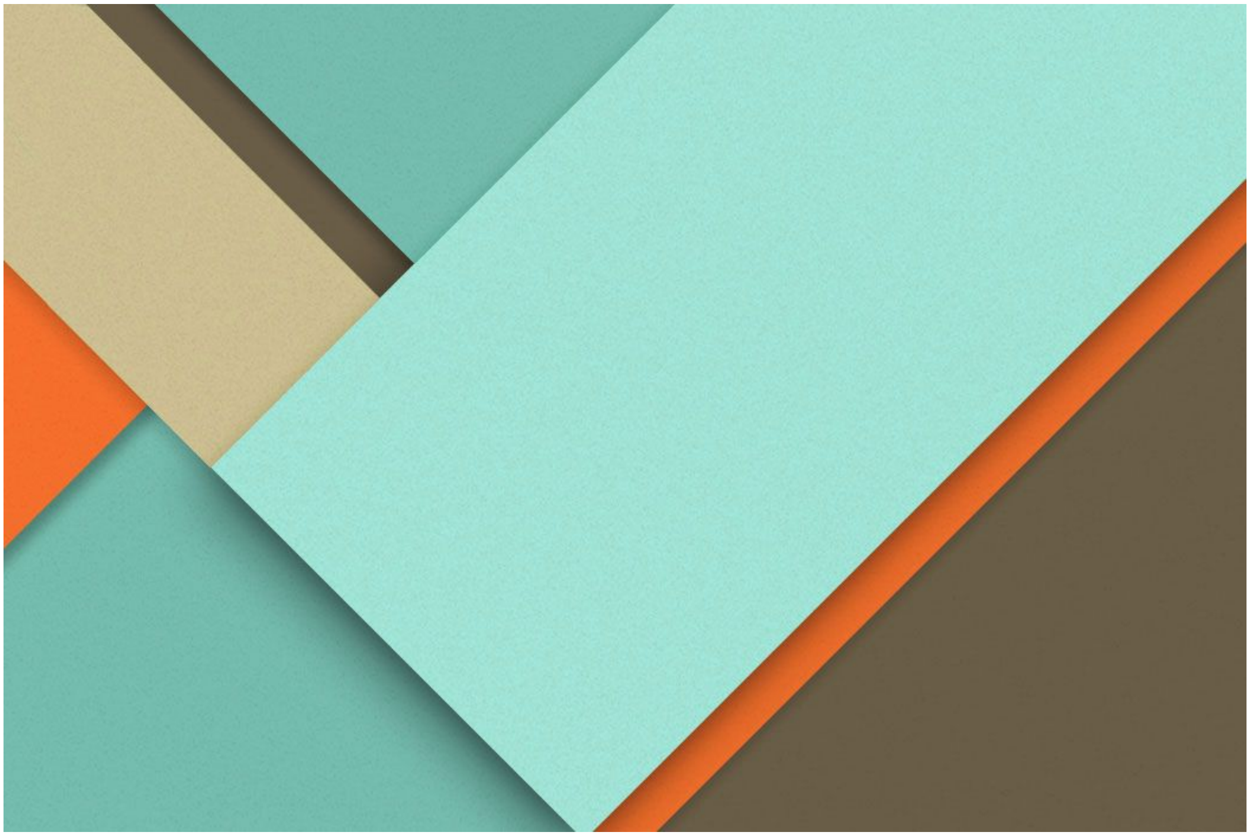


Recall Based CAPTCHA Authentication System

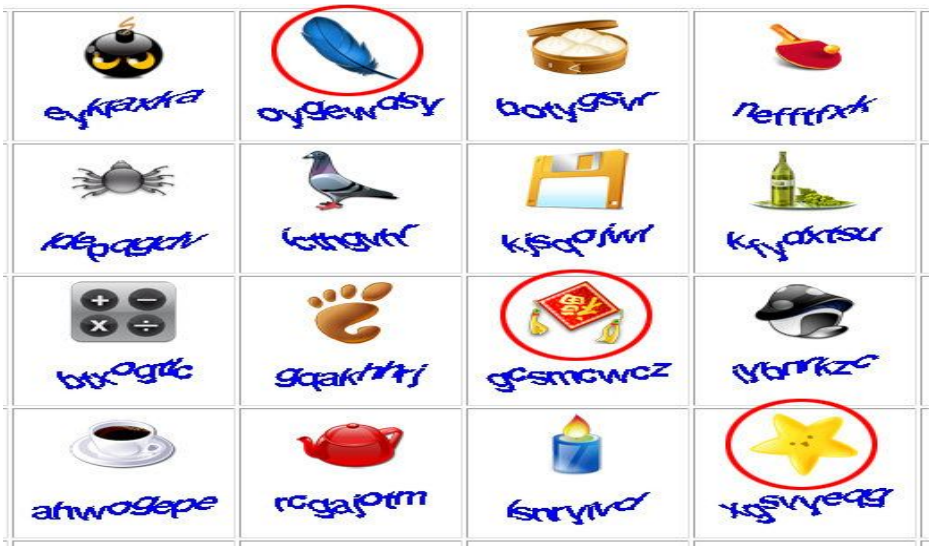
18.11.2019

Abstract

So far, of all the recall based graphical password techniques known not many are resistant to all the possible attacks.Our aim is to devise a login system that is resistant to all the possible known attacks. And we have made use of the CAPTCHA to achieve this. It is resistant to attacks like shoulder-surfing attack,brute-force attack, spyware attack, hidden camera attack.

Introduction

Basic idea is to integrate the CAPTCHA with the recognition based technique. This idea combines the ease of recognition based techniques and the security of the CAPTCHA. At the registration phase the user selects 3 pass images and for each image,a random number(pass numbers) in the range of 0 to length of captcha string. The pass images along with the respective selected numbers together generates password for every login session to the user. At the time of login user has to input the character found in the captcha of the pass image at the selected number.



Consider the above grid of images and the images circled are the pass images of a user (selected in the same as in the order of rows). And the pass numbers selected for each image be 3,1,5 all less than 8 (length of the captcha string). The password for the user for that session is *"ggy"*. The generation of password is as follows

The captcha for the pass images are

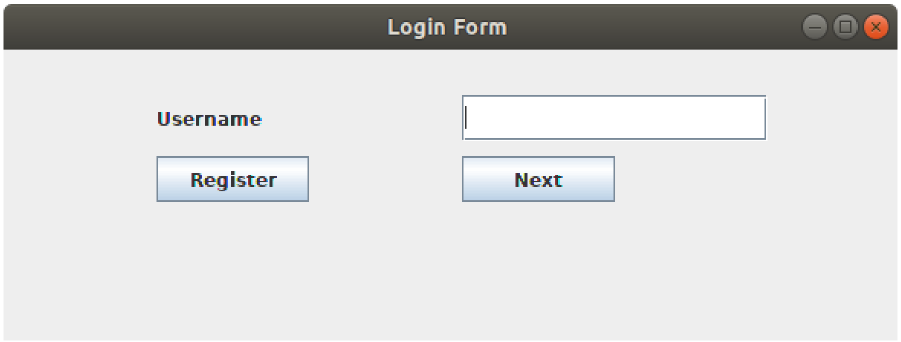
	User Selected Pass Number	CAPTCHA	Sub Password
Pass Image1	3	oygewdsy	g
Pass Image 2	1	gcsmcwcz	g
Pass Image 3	5	xgsvyeqg	y

Session Password :   ggy

The security lies in the way the password is generated for every session. Usage of CAPTCHA doesn't leave any patterns about the password as password is not constant and depends on the randomly generated string every time. The grid space along with the CAPTCHA makes it resistant from the brute force attacks.Restricting the domain in which the CAPTCHA strings are generated makes it difficult to analyze the selection pattern. Since there isn't a selection of images there is no possibility of Shoulder-surfing attack or hidden camera attack. Usage of CAPTCHA makes it spyware resistant as it is hard for machines to recognize.

Basic Working

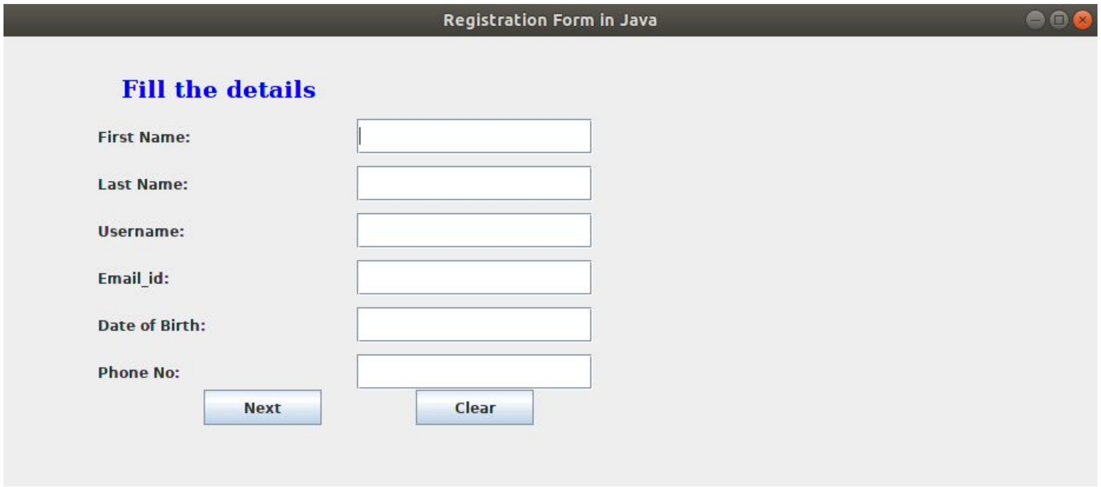
Login Form



Initially user opens our software where he needs to enter his credentials (only the username). If he is an existing user then he will proceed to the next tab where he enters his password, otherwise he needs to register. The register frame will be consisting of fields like first name, last name, username, Date of Birth (DOB). User in order to proceed to the next stage, he presses next button where he will be directed to password selection frame. User needs to select 3 images for his password selection. When he clicks each and every image, a dialog box will be popped up where the user will be entering the character number (in the range of 1-8), for selecting a position from the captcha string which is attached to the image in password page frame.

Now the registered user will be entering his username in the login form frame, where on clicking next he will be directed to password page frame.Here in this password page frame the user needs to enter the password based on his pass images and character present at selected pass number in the captcha attached to the image which were selected during password selection frame. If the password is valid then user has successfully log-in. On the other hand, if user has entered the wrong password he will be given another 2 chances for entering the correct password. If the user failed to enter the correct password then a pop up will displayed showing limit exceeded.

Registration Frame

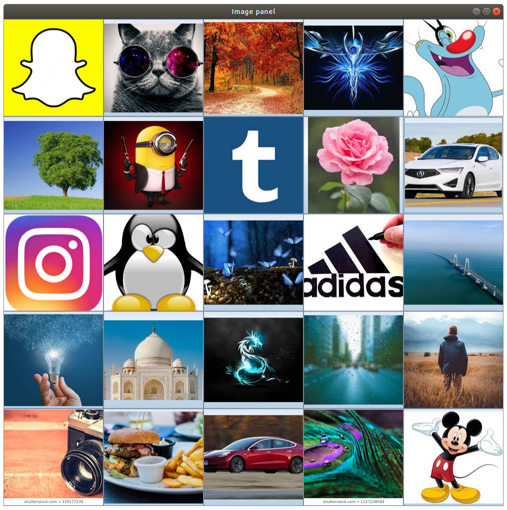


Registration Form in Java

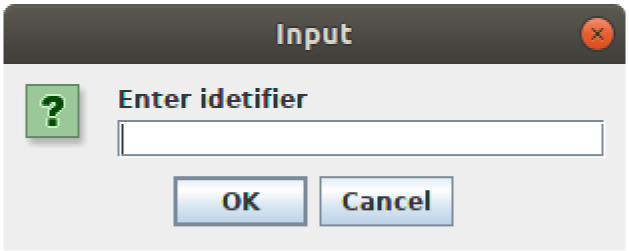
Fill the details

First Name:	
Last Name:	
Username:	
Email_id:	
Date of Birth:	
Phone No:	

Password Selecting Frame



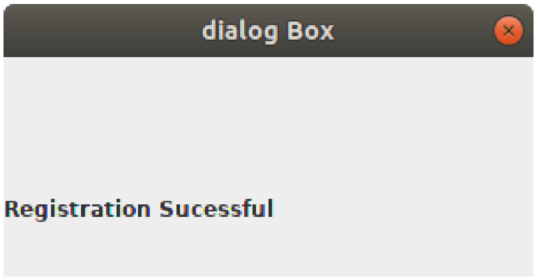
Prompting the user to select the position number for the selected image



Input

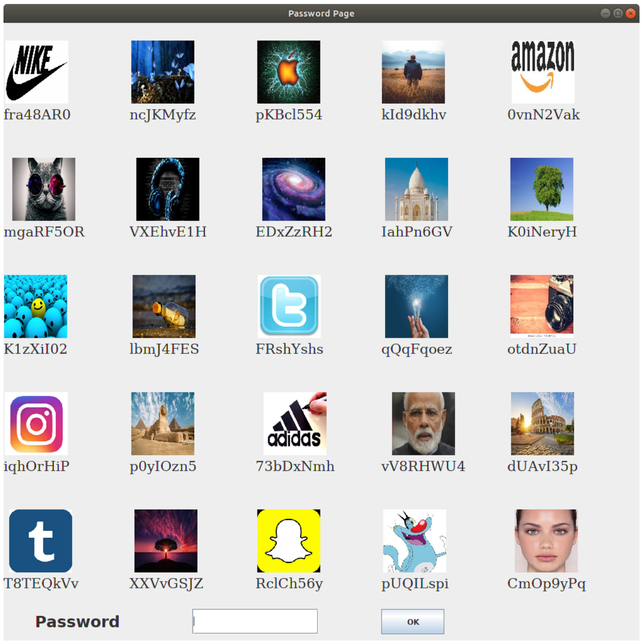
Enter idetifier

On successful registration

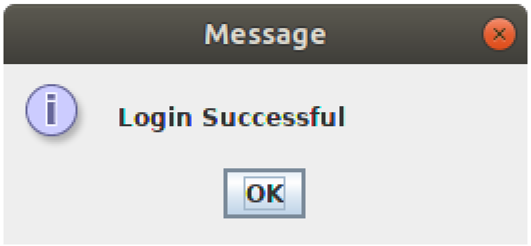


Registration Sucessful

Password entering phase:

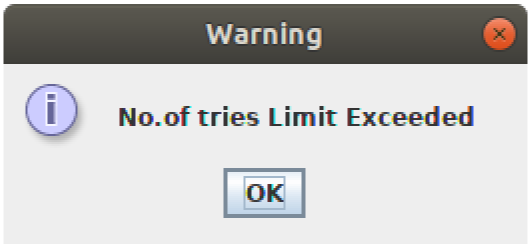


If password is valid:



Login Successful

If the user exceeds the login attempts



No.of tries Limit Exceeded

Security Analysis

I. Brute Force

Since the password is not constant and changes based on the CAPTCHA generated for every login it is resistant to brute force attack. Though the domain space of the password is constant the password is not constant for a user. It works similar to the session key which is unique for each session.

II. Hidden Camera

The point of hidden camera comes into the picture when the user selects the picture, by observing the pass images selected by the user. But here in this method user doesn't select the picture, but types the password from the CAPTCHA attached under his pass images. So, this technique is resistant to hidden camera attack.

III. Shoulder Surfing

Shoulder surfing attack is generally used to obtain person's confidential information by looking through his shoulder movement. To implement this attack the attacker does not require any technical skills, a keen observation of the victim's surroundings and his typing pattern is sufficient. With the advent of modern technologies like microphone and hidden cameras, makes shoulder surfing much easier and gives the scope for attacker for performing long range shoulder surfing attacks. In our method during the login phase, user requires to enter the corresponding captcha instead of clicking the images for password. Hence there is no scope for attacker to guess password patterns based on shoulder movement.

IV. Spyware Attack

Spyware is a software based attack where the software aims to gather information about a person or organization, sometimes without their knowledge, and send such information to another entity without the consumer’s consent. Consider the case where spyware has been installed and has noted down the password typed by the user and also recorded the password page (i.e, the pictures and the captcha). There are two strong hindrances to find the password. One is that the spyware cannot understand or analyse the captcha and the other is that since the password changes for every session one has to record a huge number of sessions and analyze every session manually to find out the password which is practically not possible. Based on these assumptions we claim that this technique is resistant to spyware attacks.

Conclusion

The above designed one is just a prototype. The future work is to quantify the security measures it can provide and finding out the key space. And further wrapping it out into a login system and try deploying it in an application.