Design and Implementation of E-Banking Authentication Algorithms for Secure Login and Transactions Using Multilevel Graphical Signatures

Mr. Bharath B M¹ Mr. T S Bhagavath Singh²
¹Student of M.Tech (CNE) ¹²Associate Prof
¹²Department of ISE
¹RNS Institute of Technology, Bangalore, India

Abstract— Many security primitives are based on hard mathematical problems. Using hard AI problems for security is emerging as an exciting new paradigm, but has been underexplored. This paper presents enhanced security architecture for application software that actually provides a multiple level of security for online banking transaction using one of novel technique called Captcha which has been most underexplored. Here there are three level of security that the application will ask to provide for the end user in order to make transaction. In second level of security is about allowing the users to solve Captcha based graphical password case. A novel family of graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CaRP) is used for this. CaRP addresses many type of security problems altogether, such as online guessing attacks, relay attacks, and if combined with dual-view technologies, shoulder-surfing attacks. Here, third phase of security is provided using the structure of sending a mail to the user with the details attached along with the image captured by the application and then allow him to access the transaction phase through the mail and then the application shutdowns.

Keywords: Graphical Password, Normal Password, CaRP, Captcha, dictionary attacks, password guessing attacks.

I. INTRODUCTION

Many security schemes available now are mostly of hardware related, that is really not a good sign for the middle level corporate companies to get access. So I planned to do some work for the security that is purely based on software rather than the hardware cost, signal issues for one time Passwords for mobile devices etc. So I thought of using the Captcha technology to provide security which is new, and it is being underexplored. CaRP is a click based graphical security scheme, where a sequence of clicks on a image is used to derive a password. So I thought of using Captcha as base in my application to provide security where it doesn't requires any type of external costs to the users.

A new security primitive based on image recognition, is used for user identification that will provide a secure way to login and for the transaction process in e-banking application. Here I like to use Captcha in different manner as textual based Captcha for login phase for the application and image based authentication for the transaction phase. Here I wished to use the Captcha to peak, to provide a better security then the present existing system like biometric, one time passwords etc that has faced some issues like hardware related issues and signal reachable issues etc. So in the proposed method, the user can simply ignore hardware related and OTP issues.

Here I used to present my application in two shades by providing multiple graphical signatures security. In first part the normal login process is applied for the users to login into the application. Later once he login another user authentication scheme based on textual graphical signatures will be used for the user to login into his account. Once he succeeded his authentication as a valid user, then he has to pass another graphical signature called image based Captcha security, that actually is done by taking the user picture and sending the details to the users mail Id. Once the user is valid user he will go to his mail, to move for the further steps in the application to transfer amount. Thus the application will provide multiple security with a cost effectiveness and very useful.

CaRP is click-based graphical passwords, where a sequence of clicks on an image is used to derive a password. Unlike other click-based graphical passwords, images used in CaRP are Captcha challenges, and a new CaRP image is generated for every login attempt.

Here in Login phase, the Captcha is displayed based on the user password and he as to select the password characters from the Captcha. That basically avoids online guessing attacks. Here Captcha is generated in such a way that, the user has provided his Captcha password at the time of registration is taken and displays his single character from his relevant password which is stored in database. The single character from his password and bunch of junk characters will be generated, once he selects his password character, the Captcha is automatically refreshed displaying another set of Captcha which consists of rest of his letters by taking one at a time. This process is done until his password matches. In second part of the application is dealing with transaction phase.

Here the user’s details are collected from the application including the picture of the user who attempt to transfer the amount and then sent across the users registered mail Id, further to continue with the process the user has to login into his mail id where the link of the application for the next step has to perform here. So this application can be used to provide multiple graphical securities that actually cost only the software and no hardware related issues etc.

Rest of the paper is structured as follows: section 2 provides an overview of an existing Captcha technology. Section 3 describes the development process of CaRP technique with its benefits over existing system. Section 4 concludes the paper.

II. LITERATURE SURVEY

Captcha has been recently labeled as one of the most underexplored technology, even though it is a novel approach of using for security concern. So I used this as one of the most important concern in my project. So I have surveyed around 25 papers of Captcha technology papers and taken 5 papers which are much related to my work.
Literature survey gives an overview of existing Captcha as Graphical Passwords. In paper [1] author has proposed a large number of graphical password schemes. They can be classified into three categories according to the task involved in memorizing and entering passwords: recognition, recall, and cued recall. This paper mainly deals with the necessity of remembering the textual passwords. Here there is a Captcha technique used where the user can easily provide his passwords by selecting the images which he chosen this basically eliminates the memorizing and entering the passwords. Authors in paper [2] provide an overview of a typical scheme is Passfaces wherein a user selects a portfolio of faces from a database in creating a password. During authentication, a panel of candidate faces is presented for the user to select the face belonging to her portfolio. This process is repeated several rounds, each round with a different panel. Here the author allows the user to select his password by providing the image of swimming pool where there are many numbers of people the user must select his password by selecting couple of people in the image.

With respect to paper [3] author uses Draw-A-Secret (DAS) was the first recall-based scheme proposed. A user draws her password on a 2D grid. The system encodes the sequence of grid cells along the drawing path as a user drawn password. Here the author provides the graphical sheet and allows the user to draw his password by selecting the points available in the graph. So that next time when he used to login he must have to provide his password by drawing his secret path in a grid that has a graph structure. This is used in 2D way. In paper [4] outlines PassPoints is a widely studied click-based cued-recall scheme wherein a user clicks a sequence of points anywhere on an image in creating a password, and re-clicks the same sequence during authentication. Cued Click Points (CCP) is similar to PassPoints but uses one image per click, with the next image selected by a deterministic function. Persuasive Cued Click Points (PCCP) extends CCP by requiring a user to select a point inside a randomly positioned viewport when creating a password, resulting in more randomly distributed click-points in a password. Among the three types, recognition is considered the easiest for human memory whereas pure recall is the hardest.

In paper [5] presents a novel based Captcha is used to protect sensitive user inputs on an entrusted client. This scheme protects the communication channel between user and Web server from key loggers and spyware, while CaRP is a family of graphical password schemes for user authentication. The paper also did not introduce the notion of CaRP or explore its rich properties and the design space of a variety of CaRP instantiations. This author basically used his technique to provide novel approach to provide the security between the communications. In paper [6] presents a reported that a significant portion of passwords of DAS and Pass-Go were successfully broken with guessing attacks using dictionaries of 231 to 241 entries, as compared to the full password space of 258 entries.

With respect to paper [7] & [8] author presents an approach Images contain hotspots, i.e., spots likely selected in creating passwords. Hotspots were exploited to mount successful guessing attacks on PassPoints: a significant portion of passwords were broken with dictionaries of 226 to 235 entries, as compared to the full space of 243 passwords.

III. CARP INTEGRATION PROCESS FOR SECURITY

The CaRP e-banking aims to provide the security to the users by providing multiple graphical signatures. It actually works under 3 different stages by which user has to pass all the stages in order to make secure transaction by using this app. The proposed system makes use of the CaRP technique in order to provide security for the 2nd stage called user authentication scheme. 1st stage a normal login phase in which the user has to provide his normal users id and password. Later in third stage image based authentication is done by capturing his image and sending his details to the registered mail id to continue the transaction phase by using this application. Thus this application is mainly deals with providing the authentication for the user by passing multiple graphical signatures in order to transfer the amount. Before actually entering into the module the new user needs to fill the registration phase as shown in simple diagram.

![Fig. 1: Registration phase basic concept](image1)

A. Normal Login Module

Any software applications contain Normal login process to make sure that the register user only has access for the application. In the same way CaRP also have normal login module in which the user must provide his normal user Id and password that makes the level1 authentication of this application. Once the user passes this phase still he is having again couple of levels of authentication that he must fulfill to Transaction by making use of this application.

![Fig. 2: Normal Login Process Basic concept](image2)

B. Carp Module

CaRP is click-based graphical passwords, where a sequence of clicks on an image is used to derive a password. Unlike other click-based graphical passwords, images used in CaRP are Captcha challenges, and a new CaRP image is generated for every login attempt. I used this which is already mentioned in [1], in different way to produce second level of authentication in the application.

Here I am making the user to apply his password from the Captcha that will appear on the screen once he passed the level 1 authentication. This Captcha is built on the user’s Captcha password given during the registration phase and allowing his to enter this as virtual keyboard facility. Here this Captcha is generated as by using some logic that actually not makes the user unhappy for long process. The logic behind this is generating the Captcha by taking the
users password from the database by character by character basis and rest all by providing the junk characters. Here is the screen shot of that which will make you to understand in a better way.

**Fig. 3: CaRP integration to the application.**

C. Image based Graphical password Module

This is second part of the application is dealing with transaction phase. Here the user’s details are collected from the application including the picture of the user who attempt to transfer the amount and then sent across the users registered mail Id, further to continue with the process the user has to login into his mail id where the link of the application for the next step has to perform here. The link that the application had sent contains enough information about the user who tries to login, so that we can easily find who has access the applicant account easily. It basically helps in keep tracking about the user who had access the account. So this application can be used to provide multiple graphical securities that actually cost only the software and no hardware related issues etc.

**Fig. 4: Application sent to the users mail id with the details along with the image who tries to access.**

D. Benefits

Proposed CaRP integration in e-banking application provides many benefits to consumer, app developers and security for the applicant account as given below:

- Consumers can extend their security to the online e-banking in a different style with the couple rounds of verification that enriches the quality of the application.
- It mainly focuses on the security, hence there are Captcha based password challenging stage as well as image based used in the transaction phase.
- It mainly reduces online guessing attacks, relay attacks, man in the middle attacks etc.
- CaRP can be applied on touch-screen devices whereon typing passwords is cumbersome, esp. for secure Internet applications such as e-banks. Many e-banking systems require solving a Captcha challenge for every online login attempt Etc.

IV. Conclusion

A new security primitive relying on unsolved hard AI problems. CaRP is both a Captcha and a graphical password scheme. The notion of CaRP introduces a new family of graphical passwords, which adopts a new approach to counter online guessing attacks etc. Paper gives an overview of CaRP integration to the e-banking application. Where the user needs to pass several level of authentication schemes in order to make transaction using this application. Once the user is registered user then he have to pass the authentication levels 1 as normal login phase. Once he cleared with this, then he has to face Captcha based entering passwords as the second level of authentication used in the application. Once he is authenticated in 2 level then if he wants to make transaction then he have to pass the level 3rd authentication where the application will capture the users image with the details of login occurrences to the user mail id, if he want to make transaction then he have to click a link sent by the application in the mail. This is more applicable because it actually reduces hardware cost for the application, OTP when there is a signal issues etc, will make this application a novel one to protect the resources with a minimal cost.

**REFERENCES**


