Randomized Image Password and a QR Code Based Circumnavigation Mechanism for Secure Authentication using caRP

R.Bhavani[#1], R.Anitha[*2]

[1]*Assistant Professor, Department of Computer Application, S.A Engineering College, Chennai, India*
[2] *Scholar, Department of Computer Application, S.A Engineering College, Chennai, India*
[1]bhavanirajajothi@gmail.com

Abstract— Password is the security primitives used for proving a user identity in online. Many graphical password techniques have been proposed which is used to improve password usability and security. In this paper, we present a Captcha as gRaphical Password (caRP) technique. caRP is used to resolve most of the security issue in graphical password such as online dictionary attacks, relay attacks, shoulder surfing attacks [1]. caRP provide new approach that address image hotspot problem which is encountered in graphical password by generate new image for each login user. User authentication has been important for security. To make secure user friendly graphical password, we use randomized image password. Randomize Image Position (RIP) randomized the visual image position of visual object [2]. To build up the security in graphical password it combines RIP and caRP. In this stage, we introduce Quick Response (QR) login mechanism to improve the security of RIP password scheme. It helps the user to securely access his account in an unsecured environment. QR means quick search and it transfer a piece of information from the transitory media to your mobile device. This scheme offers better security and well suitable for many applications.

Keywords— *Graphical Password; Security Primitive; Randomized Image Password.*

1. Introduction

Security is very important for online application. Every public network provides security by means of authentication. Usually authentication includes pair of user name and password. Authentication are divided into token based authentication, biometric authentication, knowledge based authentication.

In graphical password system, image hotspot selection and guessing attack are the major concern [3]. This conflict is resolve by using caRP technique. caRP is a click based password. In order to secure hotspot selection of an image, caRP generate new invariant image for every login, even the user login twice. To enhance the security this paper introduces RIP. The main role of RIP is to randomize a set of visual password objects and that is placed over a background image for every page reload. In order to improve security of RIP, the QR code is activated; if any user try to login via un trusted device and/or their id (such as malwares) and he/she find shoulder surfing threats. In such situation, the clicking on the password cannot be done and this scheme provides protection against malwares.

2. Existing System

This system present a secure graphical password mechanism based on the cued click point technique [4]. Cued click method is a click based scheme where users are needed to select click point on the image presented in sequence one at a time. This provide authentication for the user [5]. User can click anywhere on an image that is referred as locations [6]. While creating the password the user must remember those click points, if the selected point at login process matched with a click point at authentication process then the login attempt is successful, otherwise fails [7].

2.1 Drawbacks

- This system can mainly suffer from key loggers attack [8].
- Comparably less secure than persuasive cued click point.
- It provides less usability.
- It suffers from online guessing attack.
- Dictionary attack is feasible [9].

3. Proposed System

This paper makes authentication process to secure by using caRP, RIP and by generating QR code. In my proposed authentication, we have to select two images to authenticate. Here authentication process is purely click based. The caRP is to maintain hotspot selection of the image and so its confidential. caRP generate a new image for every login user, even the same user login two times. carp is implemented by RIP authentication. In RIP it does not maintain fixed position of password image instead it shuffle the password image position which is generated by caRP for every login users. QR code mechanism provides high level protection against malware attack and it improves the security of RIP password. In this mechanism it circulates some Intrusion Detection System (IDS) that exchange in a secured manner through mobile app.

3.1 Advantages

- Graphical password scheme provide a way of making more human friendly password.
- This system is more secure than persuasive cued click point.
- Dictionary attack is infeasible.
- It provides computation difficulties for online guessing attack.
- It improves password usability and security.

3.2 Role of caRP

caRP is a novel family of graphical password. It is a click based graphical password where clicks are the input that is used to derive the password. Shoulder surfing is one of the major security issue. Here the password is a visual object so any one who is watching the authentication can easily point out the password clicked by the user. caRP resist the issue by generate new visual object for every login attempts and the object(image) must be independent image that contain invariant information which are the user's password object.

3.3 **Authentication of caRP by using Authentication Server**

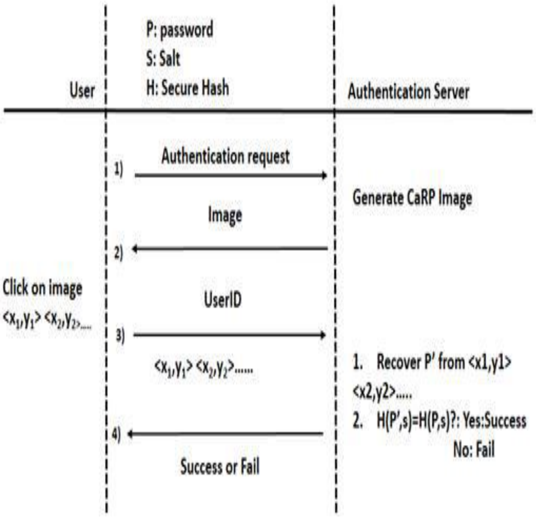
User
P: password
S: Salt
H: Secure Hash
Authentication Server
1)
Authentication request
Generate CaRP Image
Image
2)
Click on image
$\langle x_1,y_1\rangle \langle x_2,y_2\rangle$....
UserID
3)
$\langle x_1,y_1\rangle \langle x_2,y_2\rangle$......
1. Recover P' from <x1,y1> <x2,y2>.....
2. H(P',s)=H(P,s)?: Yes:Success No: Fail
4)
Success or Fail

Fig. 1: Architecture of Authenticate Server

In figure 1, authentication server (AS) provide communication between client and the server. It store unique password ID, user ID, and hash key for each user account. The password contain a set of caRP generated visual objects from that user have to click an image and then the background process convert the image into unique ID. This ID is send to AS.

Depend upon the login (client) request AS generate RIP and caRP image by randomly assigning the position of an image for each login user who have a unique set of visual object and send to client. Now user perform his second authentication by clicking the hotspot position of an image in correct sequence and that is converted into user ID's by background process and send to AS along with their user ID's. The authentications recover the hash key for the account and compute hash value of unique ID's and compare the hash value with the value stored in user account. An authentication is verified, if two values are matched.

3.4 **Circumnavigation using QR Code**

A QR mechanism is proposed to improve when the user need to access his account in an unsecure environment. There is always a chance for password leakage while using a public computer. The user may not aware of the malwares running in the background. This observation leads us to the design of an alternative login method that the user can make use of the method, when he is in an unsecured environment to enter his password.

3.5 QR Authentication by RIP Mobile App

After AS is verified the user Intrusion Detection ID is generate a QR code and send it to user. The QR code carries session ID. To extract the session ID, user has to register once using the mobile app. The mobile app has a QR reader which reads QR code and extracts the session ID. After the extraction of the session ID, the app retrieves the International Mobile Equipment Identity (IMEI) number of that mobile device and sends it to the AS for verification. After AS recovered the IMEI number, it equate with the stored IMEI number. So the authentication is success if the IMEI number is matched.

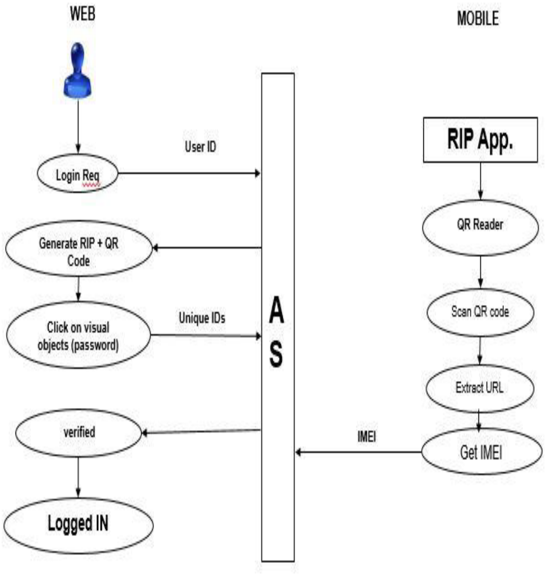

Fig. 2: Flow of RIP Mobile App

4. Mapping

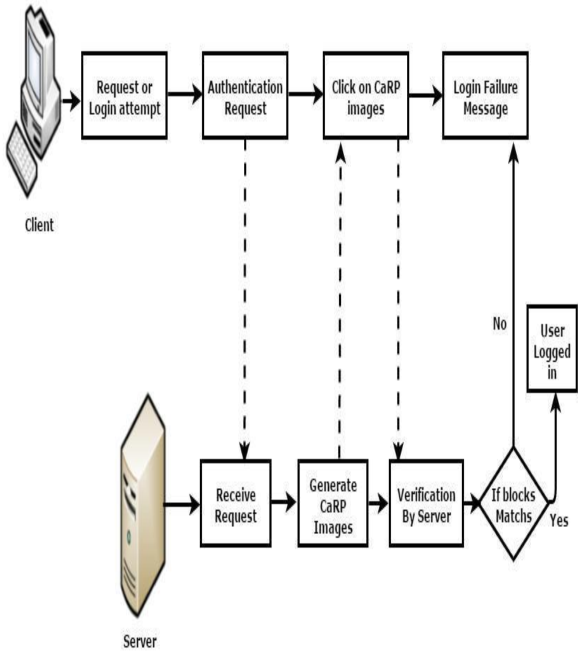

Fig. 3: Architecture of the Proposed System

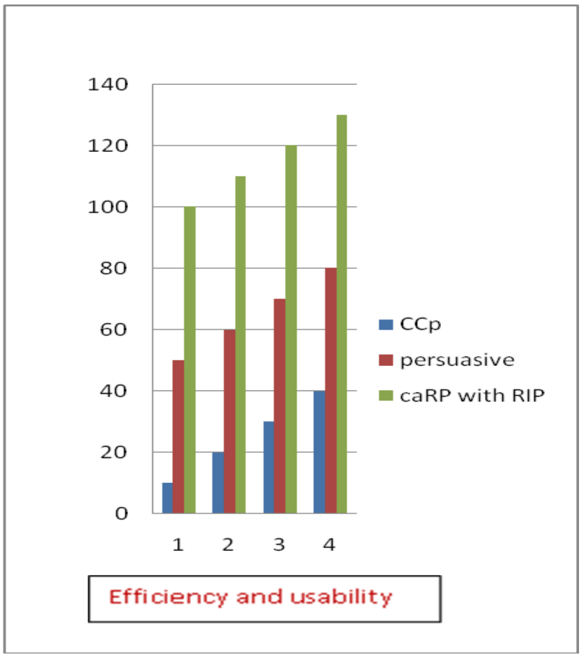

Fig. 4: Security and Efficiency of caRP

Cued Click Point (CCP) allows the user to select a click point on each image in correct sequence, thus it provide authentication to the user. The one important thing in CCP is that the user should remember a clicking position of the image. In CCP technique, hacker can easily guess the click point location of the image (hotspot). Thus it provides less security.

To enhance the security Priority-based Congestion Control Protocol (PCCP) is used. PCCP is an extension of CCP. In PCCP, the user selects an image which will divide into n part. Each part is considered as a grid from the grid user select click points. In each click point, the hotspot position is randomized. Thus it is very difficult for the hacker to find exact hotspot position. PCCP encourage user to select less predictable password and it makes user to select more difficult passwords with easy remembrances. These two techniques offer better reasonable and usability security against online dictionary attacks, online guessing attacks and shoulder surfing attacks. It provides less usability and security when we compare caRP technique.

caRP is a click based graphical password where a sequence of clicks on a caRP image is used to derive or reveal the secrete behind the image, as similar to other graphical password. The only main difference is that the caRP generate a new image for each login user, even the same user login twice. In caRP, it allows the user to select the image in authentication process that is stored in data base and user should remember the password while they are doing login. This technique secures hotspot position of the user.

Thus caRP offers usability security against online dictionary attacks, online guessing attack and shoulder surfing attacks.

5. Conclusion

In this paper, we proposed a new approach to provide security for click based graphical password. caRP is a novel approach that address image hotspot problem which is encounter in graphical password. RIP uses image randomization technique to randomly place the position of visual object over a background process. The caRP and RIP is combined to provide computational difficulty for online guessing attacks. These techniques achieved desire security for graphical password. In addition to offering protection against online guessing attack, RIP combined with QR login to resist shoulder surfing threats and attack caused by malwares. RIP is not bullet proof system. The caRP is not a final solution but offer pretty good security and fits well with many practical applications.

6. Future Enhancement

Now a day, the growth of graphical password is increased. The main advantage of graphical password is that the people can easily remember the graphical password than textual password. But the security in graphical password is very less. The caRP is a new approach that unsolved hard artificial intelligence problem and it also encounter online guessing attacks. The caRP generate a new image for each login user and it also secures hotspot position of the image.

So it is confidential and never exploit to attackers. It resists online guessing attack and inherits vulnerability in many graphical passwords. The caRP is much more costly according to human based attacks. Thus the result of my experiment shows that the future research should concentrate on improving the login time and memo ability of a user.

- Can be used for secure transactions in e-banking.
- Cross device Authentication.
- Spam mitigation.

References

[1] Bin B. Zhu, Jeff Yan, GuanboBao, Maowei Yang, and NingXu, CAPTCHA as Graphical Passwords—A New Security Primitive Based on Hard AI Problems‖, IEEE transactions on Information Forensics and Security, Vol. 9, no. 6, June 2014.

[2] Dhamija, R. and A. Perrig, 2000. Déjà vu. A User Study Using Images for Authentication, SSYM'00 Proceedings of the 9th conference on USENIX Security Symposium - Volume 9, Denver, Colorado — August 14 - 17, 2000, Pages 4-4

[3] Haitao, Pass Go, a New Graphical Password Scheme‖, Master Thesis, University of Ottawa Canada, June 2006.

[4] L.Sobrado and J.C. Birget, Graphical Passwords, The Rutgers Schloar, An Electronic Bulletin for Undergraduate Research, vol 4, 2002 .

[5] FarnazTowhidi , Maslin Masrom , A Survey on Recognition-Based Graphical User Authentication Algorithms, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 2, 2009, pp. 119-127

[6] P.Dunphy and J.Yan, Do background images improve Draw-a-secret' graphical passwords, CCS '07 Proceedings of the 14th ACM conference on Computer and communications security, Alexandria, Virginia, USA, 2007, Pages 36-47

[7] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, PassPoints: Design and longitudinal evaluation of a graphical password system,‖ Int. J. HCI, vol. 63, Jul. 2005, pp. 102–127,

[8] R. Biddle, S. Chiasson, and P. C. van Oorschot, Graphical passwords: Learning from the first twelve years, ACM Comput. Surveys, vol. 44, no. 4, 2012.

[9] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, The design and analysis of graphical passwords,‖ in Proc. 8th USENIX Security Symp., 1999, pp. 1–15.