Indian Journal of Science and Technology, *Vol 8(26), IPL0492, October 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Online Guessing Attacks – A Prevention using PGRP and PCCP

Ushus Elizabeth Zachariah[1]*, R. M. Swarna Priya[1] and V. S. Dharun[2]

[1]VIT University, Vellore - 632 014, Tamil Nadu, India; ushus@vit.ac.in, swarnapriya.rm@vit.ac.in
[2]Noorul Islam University, Kumaracoil, Kanyakumari – 629180, Tamil Nadu, India; dharunvs@yahoo.com

Abstract

Background: Cryptanalytic attacks like Brute Force and Dictionary Attacks over password-only remote login services are widespread now-a-days. The major challenge is to allow the genuine users to login by preventing such attacks. **Method:** PGRP (Password Guessing Resistant Protocol) and PCCP (Persuasive Cued Click Points). **Results:** It gives a security mechanism for preventing the fraudulent user from using the system and also tries to identify the details of fake user. **Application:** User Authentication Based Systems

Keywords: Authorization, Dictionary Attacks, Online Attacks, Password Protection

1. Introduction

The password based systems has the threat of online guessing attacks and this is very common in web applications. The major attacks are brute force and dictionary attacks. The brute force attack is one in which the user passcode or PIN is guessed by trial and error. Some automated systems are used to generate various combinations of the passcode. This is a very common attack which is used by criminals to decrypt a data. Dictionary attack[1] is one by which the password is broken in the system by the usage of the words in the dictionary.

These kinds of attacks are prevented by various techniques. The most popular one is locking of the user account if the password goes wrong for more than some attempts or by asking some secret questions with the help of an Automated Turing Tests (ATTs), Reverse Turing Tests (RTTs)[2] and Captcha[3]. The most popular ATTs are Pinkas and Sander (PS)[4] and Van Osrdchot and Stubblebine (VS)[5].

This work discusses a methodology which is followed to increase the security of login based systems by the usage of Password Guessing Resistant Protocol (PGRP)[6] and Persuasive Cued Click Points (PCCP).

The rest of the paper is organized as follows. The section 1 describes the methodologies used. The section 2 gives the implementation architecture and the next section discusses the results.

2. Methodologies Used

2.1 PGRP

This is a login protocol[1] whose main objectives are as given below.

1. The brute force and dictionary attacks need to be prevented.
2. The deployment and scalability of the protocol has to be easier.
3. The protocol should not be decreasing the usability of the users.

The protocol is designed to use the IP address, cookies or both to identify the systems using which the user logs in for the first time for the purpose of registering for authentication.

*Author for correspondence

2.2 PCCP

This is an image authentication technique. The technique is as follows

During Registration

1. A list of various images are displayed and any one of the image is selected.
2. From the image selected an articulation point is given by the user and the (x,y) co-ordinates are stored.

During Authentication

The image which is selected and the articulation point are matched with the one given during registration.

3. Implementation

The architecture Figure 1 involves the system administrator creating the account for a new user. The user is then intimated with the details such as username, password, account number, etc. later. Upon successful login, the user is granted access to his/her account where he can perform tasks like check current balance, transfer amount from his/her account to another account, etc. Here, amount transfer is accomplished by a unique Transaction ID for each transaction that is sent to the user's registered Email ID. In case of a failed login, the PGRP (Password Guessing Resistant Protocol) mechanism is activated and ensures that ample re-login attempts are given to legitimate users. The number of attempts given to illegitimate users are less. If the user is still unable to access his/her account, he/she is redirected to the PCCP[8] (Persuasive Cued Click Points) page where he/she is required to input the accurate coordinates for the picture uploaded by him/her for added security. If the coordinates entered are correct, account access is granted, else the user is redirected to a fake user login.

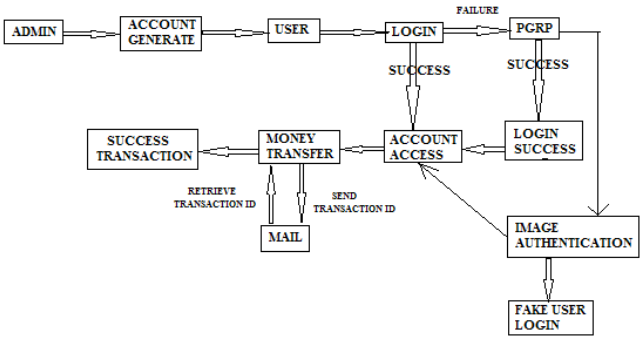

Figure 1. Architecture of the System.

4. Results and Discussion

The implementation is associated with E-banking scenario. The system flow is as discussed below.

1. The admin creates the new user account and registers the same
2. The user activates his account using the username and password provided by the administrator Figure 2.
3. The system registers the IP address from which the user logs in to activate.
4. The user is also requested to register for the image authentication.Figures 3, 4
5. Then the system follows all the kinds of activities which a banking software will do like account information, transfer of funds, etc.

The security is increased when compared to the other available systems. There are 3 levels of security provided.

1. The user when logins for the first time, the IP address (Figure 5) of that system along with username and time is stored in the database. If the user logins from the same IP address[7] the next time and forgets his password, he would be given 5 login attempts (Figure 6) before re-directing to PCCP page. If the user logins from a different IP address the next time and forgets his password, he would be given 2 login attempts before redirecting to PCCP page.
2. The correct image and its (x,y) co-ordinates are verified for a particular user. Here, he is shown 6 images out of which 5 are random and the 6th is the image (Figure 7) that was uploaded by the user initially. If the wrong image is selected, the user is redirected to the homepage but if the correct image is selected, the user is redirected to the image page where he can select (x,y) co-ordinates (Figure 8) of the point on the image.

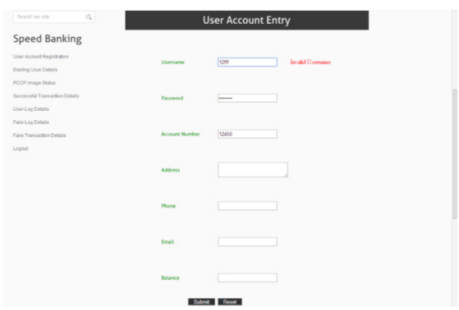

Figure 2. User creation screen.

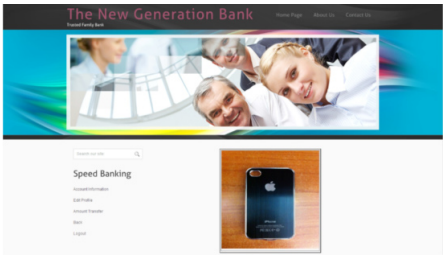

Figure 3. Image upload by user.

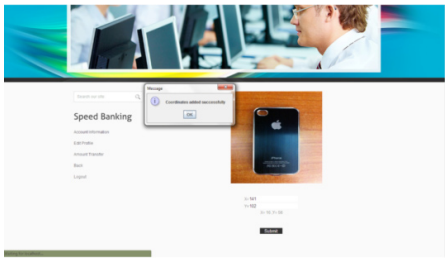

Figure 4. (x,y) Co-ordinates selection.

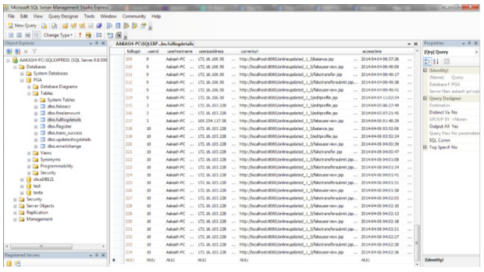

Figure 5. IP address retrieval in DB.

Figure 6. User Login.

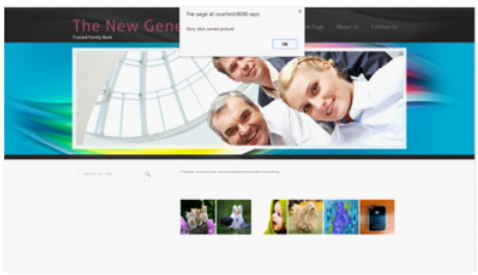

Figure 7. Image selection from the list.

3. The user if wants to change his email address (Figure 10), then an email is sent (Figure 12) to the already registered address which has a code and if the code is entered (Figure 11), the email is allowed to be updated (Figure 13) which is the final level of authentication provided if in case both the first two levels fail and the fraudulent user tries to transfer money. If the code doesn't match, the fraudulent user is redirected to a fake page which is similar to the actual one.

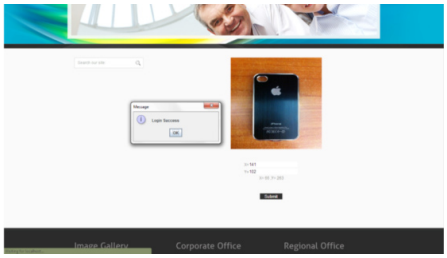

Figure 8. Image co-ordinates correct.

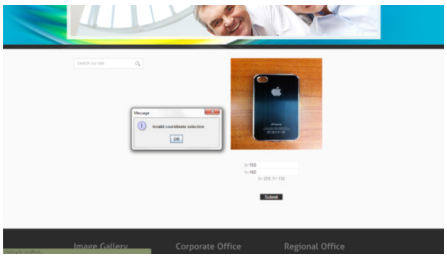

Figure 9. Image co-ordinates mismatch.

Figure 10. E-mail change request

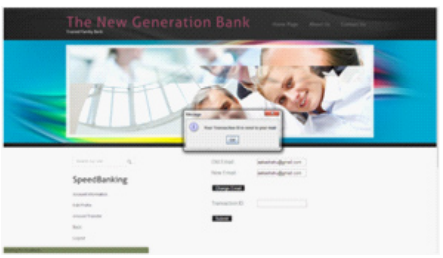

Figure 11. Transaction code request.

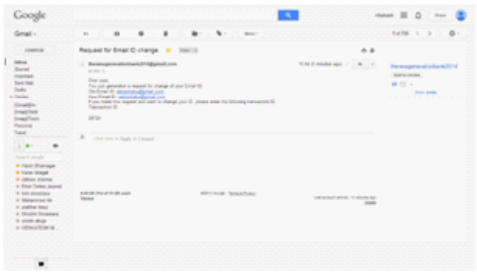

Figure 12. E-mail with code.

Figure 13. Code matched & Email updated.

5. Conclusion

Most of the security mechanisms provide only technique to prevent the unauthorized access. The system which is discussed here, apart from preventing, it also tries to identify the fake user and the administrator gets details of the unauthorized user. This helps in warning the authorized user and to get secured.

6. References

1. Narayanan A, Shmatikov V. Fast dictionary attacks on human-memorable passwords using time-space tradeoff. Proceedings of ACM Computer and Comm Security (CCS '05). 2005 Nov; p. 364–72.
2. He Y, Han Z. User authentication with provable security against online dictionary attacks. J Networks. 2009 May; 4(3):200–7.
3. Ahn LV, Blum M, Hopper N, Langford J. CAPTCHA: Using hard AI problems for security. Proc Eurocrypt. 2003; 2656: 294–311.
4. Pinkas B, Sander T. Securing passwords against dictionary attacks. Proceedings of ACM Conf Computer and Comm Security (CCS '02). 2002. p.161–70.
5. Oorschot PCV, Stubblebine S. On countering online dictionary attacks with login histories and humans-in-the-loop. ACM Trans Information and System Security. 2006 Aug; 9(3):235–58.
6. Alsaleh M, Mannan M, Oorschot PCV. Revisiting defenses against large-scale online password guessing attacks. 2012 Jan-Feb; 9(1):128–41.
7. Casado M, Freedman MJ. Peering through the Shroud: The effect of edge opacity on Ip-based client identification. Proceedings of Fourth USENIX Symp Networked Systems Design and Implementation (NDSS '07). 2007; p. 13.
8. Chiasson S, Stobert E, Forget A, Biddle R, Oorschot PCV. Persuasive cued click-points:design, implementation, and evaluation of a knowledge-based authentication mechanism. 2012 Mar-Apr; 9(2):222–35.