International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

CaRP For User Authentication System Using Mobile Interface

Walanjkar Dipika Dattatraya[1], V. S. Nandedkar[2]

[1] Department of Computer Engineering, PVPIT, Bavdhan, Pune, India

[2] Professor, Department of Computer Engineering, PVPIT, Bavdhan, Pune, India

Abstract: ***Many security techniques are used for authentication of user. Text based passwords are used by many users for their authentication. But the security as at high risk when using text based passwords. Graphical passwords are another way to authenticate user. So in this paper we are introducing the security technique related to AI problem. Captcha is used to create the graphical passwords. Means puzzles can be given to the user at the time of login process. But there are also chances of attacks on graphical password such as eavesdropping, shoulder surfing attacks etc. To overcome the drawback of graphical password and also to provide more secure approach, this paper introduces the mobile interface. In that the random questions are sent to the user's mobile then user will give the answers to the questions which he has been asked during the registration process. Due to this, even if the graphical password is intercepted but the interceptor is not able to give the answer because questions are send only to authorize person's mobile.***

Keywords: Graphical Passwords**,** AnimalGrid, Random Question Generation, Security Primitive, CaRP.

1. Introduction

There are many security related problems when using the text based passwords because text based passwords are easy to guess. The interceptor can guess the text based password by making combinations of letters, also can guess by personal information of user such as mothers name, children's name, birth date etc., these type of attacks are called as dictionary attacks and eavesdropping attack. To overcome the drawback of text based passwords the graphical passwords are introduced.

In the graphical password the user can click on different points on same image or different images. Graphical passwords are divided into three types: Recall based, Recognition based and Cued Recall based. Recall based graphical passwords are called as draw metric passwords. In the recall based graphical password the user draw the secrete drawing on the plane canvas which is divided into the grid format. On that grid the user draws the pattern which he has to remember during the login process. Draw A Secret (DAS) and Pass-Go are the examples of the recall based graphical passwords.

Recognition based graphical passwords are called as cognometric passwords. Here the different images of people, animals are given in grid format where each grid contains the different image of people and animals. During the registration process the user will select the some images from the set of images as his/her password. Then at the time of login the user has to recognize the same images from the set of images which he has selected during the registration process. The Passfaces and story system are the techniques used in recognition based graphical passwords.

Cued recall based graphical passwords are also called as locimetric because in this type of graphical passwords the user has to select the different locations on the image, and has to remember all the locations during the login process. All the types of passwords which are discussed above are all vulnerable to the security attacks such as shoulder surfing, phishing, eavesdropping attacks. In this paper, captcha is used for graphical passwords. The use of captcha as a graphical password reduces the chances of online dictionary attacks, because the user cannot make the different combinations of images as compared to text based captcha.

Also by using captcha as graphical password, the system is protected from relay attacks, because different combinations of images are given at each login. The applications where captcha as a graphical password is used are:

1) The captcha as graphical password is used in many internet applications specifically in the e-banking applications, where user has to solve the different captcha at each login.
2) By using the captcha as graphical password the entry of spam emails are reduced. Here the email service provider uses the captcha as graphical passwords to log in the system so the spam bots cannot logged into the system because they are not able to solve the captcha.

2. Related Work

A number of techniques are used from the years for Captcha. First the captcha developed is text captcha [2], in the text based captcha the alphanumeric characters are displayed on the screen. In the text based visual challenges are given to the user to identify the alphanumeric characters. Text captcha is commonly used to identify human from robots. The next type of captcha is image captcha where the image is displayed on users screen, on which user will click on different images. The drawback of this type of captcha is user cannot click on arbitrarily on the background of image. Now a day's Captcha is used for graphical password. Using the captcha as graphical password the drawback of text based captcha is overcomes.

Many techniques are used for graphical passwords. A typical recognition based scheme is Passfaces [2] where a user will

select the images from different portfolio images. The login is successful when user selects the images at each round. The images in the panel remain same but positions are exchanged. Another recognition based scheme is Story [2], this scheme is same as Passfaces scheme but the users has to select the images in same order like a story. The AnimalGrid [1] and Text4CR [1] are the techniques based on recognition based and recall based schemes. These methods are used to overcome the attacks like relay, online dictionary etc. These methods are better at remembering than text passwords. Drawback of these methods is if the attacks on CaRP then there are no any technique discussed. Draw A Secrete (DAS)[2], Pass-Go, Passfaces, Passpoints, Story Scheme [3] etc. These are the all the simplest methods of graphical passwords. A number of techniques are used from the years for Captcha. First the captcha developed is text captcha[1][2], in the text based captcha the alphanumeric characters are displayed on the screen. In the text based visual challenges are given to the user to identify the alphanumeric characters. Text captcha is commonly used to identify human from robots.

The next type of captcha is image captcha where the image is displayed on users screen, on which user will click on different images. The drawback of this type of captcha is user cannot click on arbitrarily on the background of image. Now a day's captcha is used for graphical password. Using the captcha as graphical password the drawback of text based captcha is overcomes. Many techniques are used for graphical passwords. A typical recognition based scheme is Pass faces [2] where a user will select the images from different portfolio images. The login is successful when user selects the images at each round. The images in the panel remain same but positions are exchanged. Another recognition based scheme is Story [2], this scheme is same as Pass faces scheme but the users have to select the images in same order like a story. The AnimalGrid [1] and Text4CR [1] are the techniques based on recognition based and recall based schemes. These methods are used to overcome the attacks like relay, online dictionary etc. These methods are better at remembering than text passwords. Drawback of these methods is if the attacks on CaRP then there are no any technique discussed. Draw A Secrete (DAS)[2], Pass-Go, Passfaces, Passpoints, Story Scheme [3] etc. These are the all the simplest methods of graphical passwords.

The Ant Colony algorithm [6] is used to display the any two random questions from set of questions from the databases. Questions are randomly generated for each client. By using this algorithm the according to the security level the questions are sent to the users mobile. The algorithm is used to retrieve the random questions from the set of questions faster. Short Message Service is way to send messages to users mobile. The messages which are going too sent to the user's mobile are first stored at database and the forwards to the users mobile same mechanism is used to send messages from user to system.

The SMS gateway [5] is used to send SMS to users mobile, while doing this the device save the SMS at database, transform the message to users mobile by encrypting message so that no interceptor can intercept that message. SMS gateway is used to send the messages to mass or bulk of clients. This technique of sending SMS to user's mobile using SMS gateway is reliable and faster. So the sending SMS to user from system database and receiving answers from user to system in the form of SMS is done by using the SMS gateway.

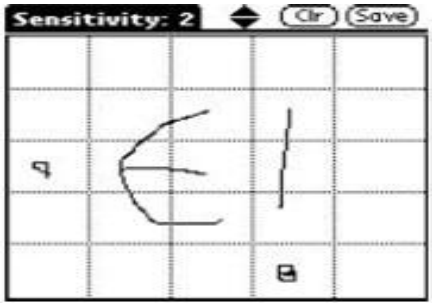

Figure 1: Draw A Secrete (DAS)[2]

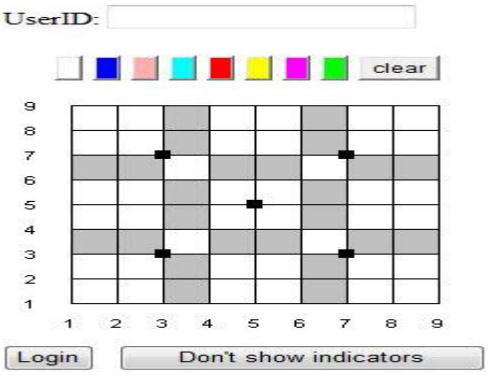

Figure 2: Pass-Go [3]

3. Proposed System

The system uses the Animal Grid [1] method for the creation of graphical password. In this the grid is created, the gird is of size (9 × 9). In the each cell the image of different password scheme which is combination recognition and recall based graphical password. Also there are chances of attacks on graphical password also such as denial of service attacks, relay attacks, eavesdropping attack etc. To overcome the system from these types of attacks, the system uses another level of authentication after choosing password from animal grid. The random question generation technique is used. We discuss the system in remaining sections.

3.1 System Architecture

As shown in the below fig.3 the system will work as follows:

a) Registration Process

1) First user starts the registration process, where he will select at least 6 images from animal grid. The animal grid image is generated by system from the system's database.
2) Then the selected graphical password by user is saved in database.
3) Then the user asks to answers set of 10 questions. User has to give answers to these questions. Answers also saved into system database.
4) Registration process is completed here.

b) Login Process

1) During login process first step is user enters the username and selects the image which he has selected during registration process.
2) Then user selects the images from animal grid. If the selected sequence of images are stored sequence then only user can logged into system. Otherwise login will fail.

c) Transaction Process

1) After successful login user will actually enters into the system where he can do transaction.
2) For that transaction user will enter details when he submit his transaction at that time two questions are send to the user's mobile .
3) When user gives correct answers to these questions then only transaction is successful otherwise not.
4) In this step user is given two chances two answer the questions. If in both chances he give wrong answer then user cannot do the transaction.

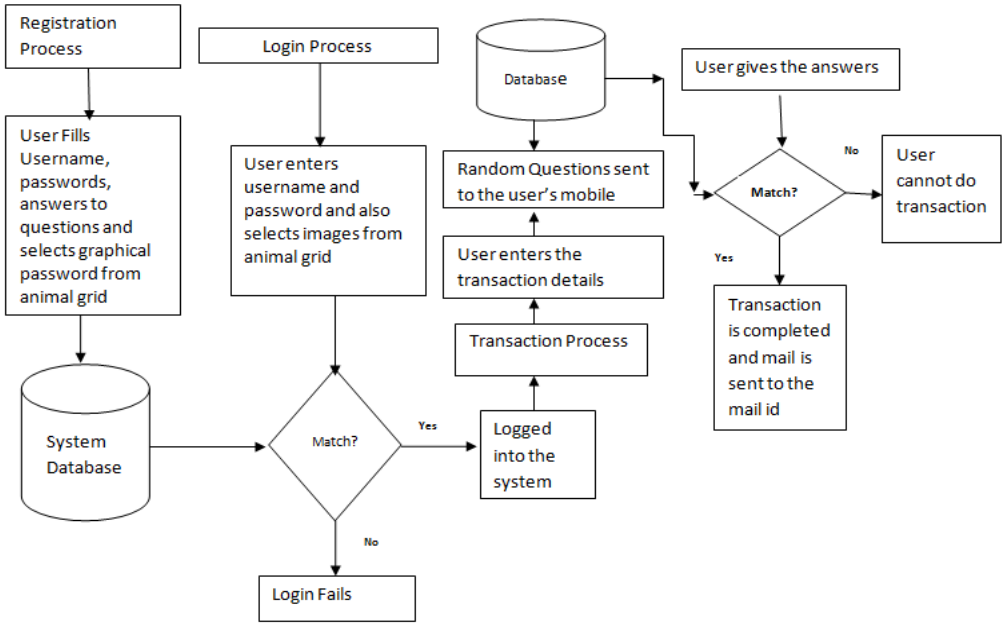

Figure 3: System architecture

3.2 Animal Grid

The Animal Grid is used as the first step of authentication process. In this, the grid is created of size (9 × 3). In each grid the images of different animals are displayed. Changes to this module from suggested animal grid [1], we are again divide 3 cells into four parts. As shown in fig. 4. From that user will select the at least six images

Figure 4: Animal Grid

3.3 Random Question Generation

This step of our extended system architecture is used when user will think that his password is intercepted by the interceptor. So in transaction process this module will help to secure the system from the interceptor. In this step the system will generate the random questions and are sent to the user's mobile. So even if password of user is stolen the interceptor cannot do any transaction in to the system because this level of security is not known to the interceptor. Also when user is not in the login process even if user gets message from the system of random questions the user will know that somebody is login into the system instead of him. So the user can change the password by selecting different images from the animal grid. Here for random question generation the utility based agent algorithm [4], and ant colony algorithm is used [6].

3.4 Mobile Interface

The random questions generated by system are sent to the user on his mobile. Here the mobile interface is introduced. For sending the message to the mobile SMS gateway [5] is used. SMS gateway is a device or service offering SMS transit; transforming messages to mobile network traffic from other media, or vice versa, allowing transmission or receipt of SMS messages with or without the use of a mobile phone.

3.5 Mathematical Model

The mathematical model used for proposed system is shown below:

1) Let system S={ R, L, Cp, IP, Q, A, U }
2) R is registration process=I fill, IP1, Cpk, A
3) If user want more security then,
4) Answer the questions
5) A= { a1, a2, ..., a15 }
6) Questions generated by Server
7) Q= { Q1, Q2, Q3, ... }
8) L is login process which depend on R= {U, IP2, Cpp, q, a}
9) U is user = {u1, u2, . . ., un }
10) If IP1=IP2 Where, IP is Image Password= {IP1, IP2, IP3. . . IPn}
11) User click on animal Grid image
12) If Cpk = Cpp
13) K and p =1. . . . . n Where Cp generated by user click point on animal grid={Cp1,Cp2. . . Cpn}then select questions and send random questions on mobile, where
14) q is ⊆ of Q
15) a={ans1, ans2}
16) a⊆ A
17) If all condition true Then login successful
18) Else Login fails. . .

4. Results

4.1 Snapshots

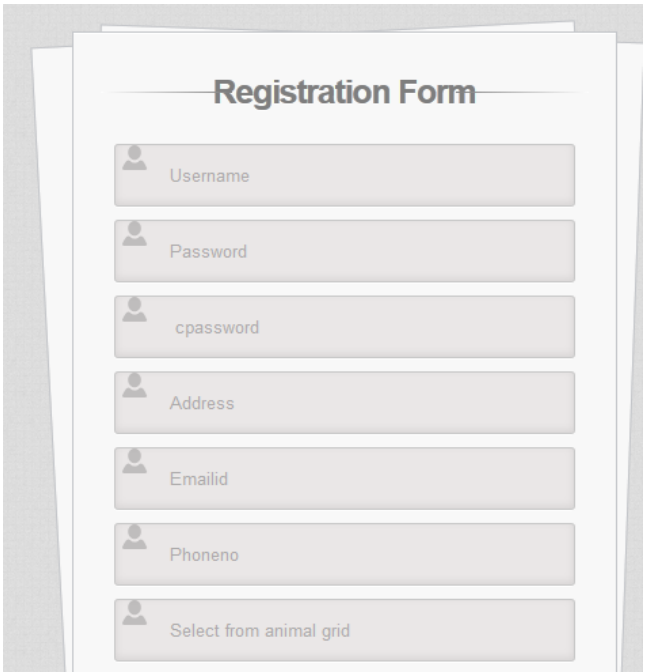

Figure 5: Registration Process_1

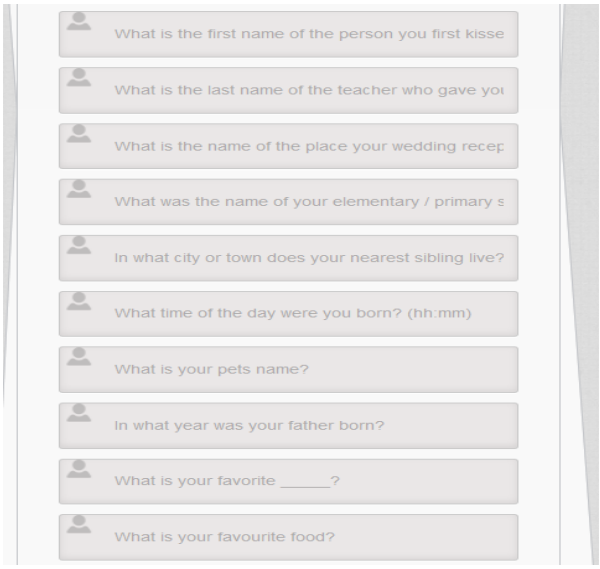

Figure 6: Registration Process_2

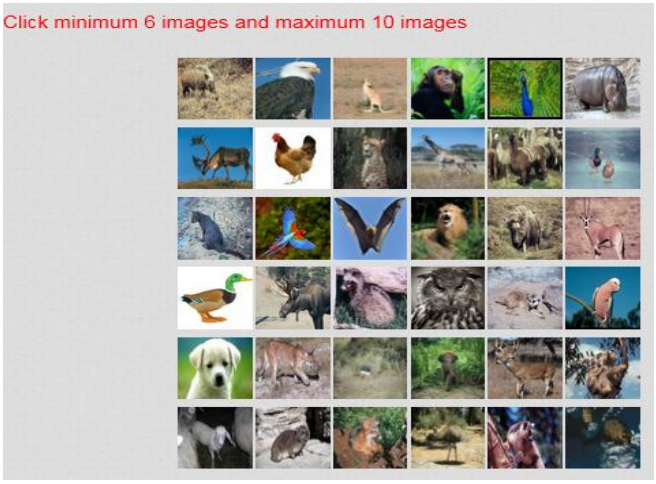

Figure 7: Registration Process_3

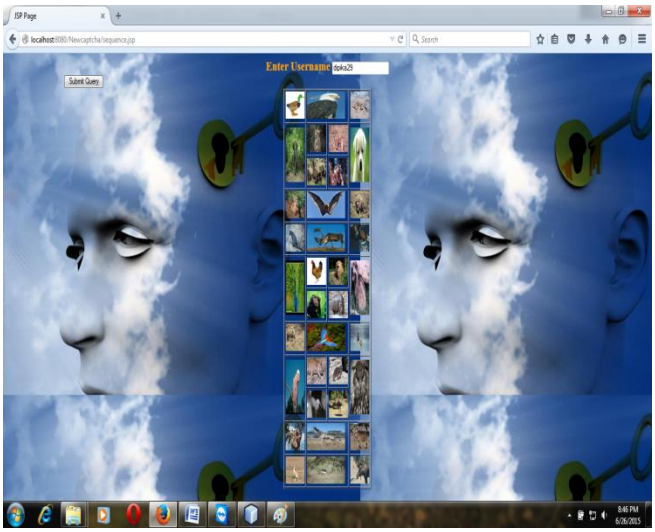

Figure 8: Login Process

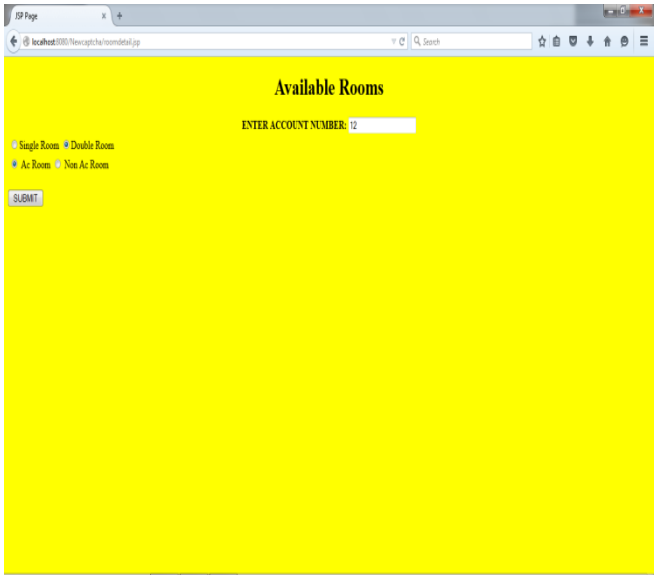

Figure 9: Transaction Process

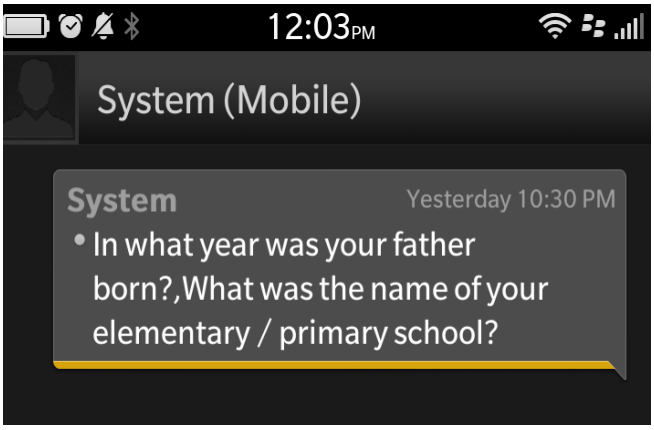

Figure 10: Random Questions are sent to the user's mobile

Figure 4: Answers are given to the question sent to the mobile

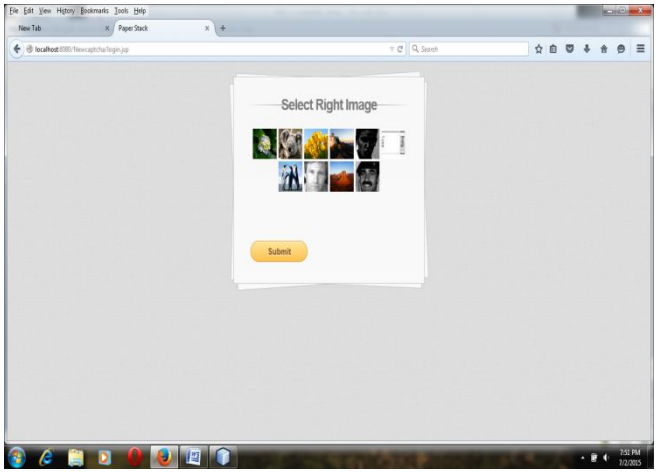

Figure 11: Level of Security

As shown in Fig.5,6,7 Registration Process is done where user selects username, text password, one image, password using animal grid, and answers the 10 questions. After that as shown in fig.8 login process is done where user enters the username and password using animal grid. In transaction process (fig.9) user enters the account details and selects the room which he/she wants to book. When user clicks on submit button, any two random questions are sent to user's mobile (fig.10). After this user will give answers to the questions (fig.11), if user give wrong answers then the again two different questions are sent to the user's mobile again if user give wrong answer then session is expired. If the user give right answers then the level of security is added to user's transaction (fig.12) where user has to select the right image which he has already selected during the registration process. This is how the system works.

4.2 Comparison

If we use only animal grid as an authentication technique to overcome the drawbacks on text based passwords then it is helpful in some time. But if any observer is sitting near us when we select the images on animal grid then it is easy for observer to intercept the password. So to avoid such type of attacks our system uses one module which is random question generation. Using this module even if interceptor enters into the system he/she cannot do any transactions in the system. That is the chances of attacks on our system are least as compared to previous system.

5. Conclusion

Captcha as graphical password authentication system is developed by graphical password based on animal grid method which uses both the combination of recall based and recognition based systems. Our system provides animal grid from which user will select his graphical password. There are chances of attacks on graphical password also such as eavesdropping attack, denial of service attack relay attack. To overcome this type of attack, the proposed system uses the random question generation. Where the generated questions are sent to the user's mobile. So only user can answer that questions not the interceptor. So even if the password is stolen by interceptor, the proposed system will not allow the interceptor to do transactions into the system until correct answers of random questions

References

[1] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang and Ning Xu , "Captcha as Graphical Passwords- A new security Primitive Based on ard AI Problems," IEEE Transactions on information technology forensics and security, Vol. 9, No. 6, June 2014.
[2] R. Biddle, S. Chiasson, and P.C. van Oarschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Surveys, Vol. 44, No. 4, 2012.
[3] Rosa Lin, Shih Yu Huang, Graeme B Bell, Yeuan-Kuen Lee, "A new Catcha inteface design for mobile devices ," Dept. od CSIE, Ming Chaun University, 5 Tech-Ming Rd, Guei-Shan, Taiwan 333,2011.
[4] Memoona Naz, M. Aslam and Ehteshan-ul-haq Dar, " Utility Based Agent For Test Paper Generation," Inernational Jouranal of Multidisciplinary Sciences and Engineering, Vol. 1, No. 1 , Sepetember 2012.

[5] Veena K. Katankar, Dr. V. M. Thakare, "Short message service using SMS gateway," (IJCSSE) Internation Journal on Computer Science and Engineering, Vol. 02, N0. 04, 2011, 1487-1491.
[6] Dan Liu, Jianmin Wng , Lijuan Zheng," Automatic Test Paper Genaeration Based on Ant Colony Alogorithm," Journal of Software, Vol. 8, No. 10, October 2013.
[7] (2012), Feb). The science behind Pssfaces[Online]. Available: http://www.realuser.com/published/ScienceBehind Passfaces.pdf.

Author Profile

Walanjkar Dipika Dattaraya student of ME Computer Engineering second year from the college TSSM's Padmabhushan Vasantdada Institute of Technology, Bavdhan, Pune.