International Journal of Emerging Engineering Research and Technology
Volume 2, Issue 7, October 2014, PP 136-141
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

M-Banking Using Persuasive Cued Click Points

Supriya Ghadge [1], Snehal Kate [2], Vaibhav Mohite [3], Shweta Patil [4]

Computer Engineering, RMDSSOE, Pune, India
[1]*supriyaghadge1125@gmail.com*, [2]*snehalkate1612@gmail.com*, [3]*vaibhavmohite688@gmail.com*
[4]*shwe221994@gmail.com*

Abstract: *This paper presents M-banking using persuasive cued click points which provide high level of security. An important goal of the authentication system is to provide support to users in selecting better passwords thus increasing security by expanding password space. The use of click based pass words leads to the selection of passwords which can be easily hacked. We use persuasive technique to influence the user in selecting the password in random manner rather than using a particular sequence. Our method significantly reduces the drawbacks of the current authentication method that is being used.*

Keywords: *Persuasive, Authentication, Cued, Pass point, Android App*

1. INTRODUCTION

The problems of using knowledge based authentication are well known. The knowledge based authentication system includes the text passwords, biometric methods and graphical passwords. Users often have their text passwords which are easy to remember. Hence these methods prove an easier way for the hackers to trace the password by using several hacking techniques available. The use of text password scheme is definitely difficult for the users to remember, because in order to provide the better security users may use different text passwords for their purpose. In such cases, it will be difficult for the user to remember the passwords that is being used for the applications.

The password authentication system that we use should provide strong passwords and also making it easy to remember. In the click-based password scheme, poorly chosen password will lead to emergence of hotspots-portion of the image where the users are more likely to select the click points. This makes it easy for the hackers to find the password scheme easily in an image.

To overcome all these existing defects we provide an authentication scheme in which selecting the password scheme plays a vital role. This method also provides a more secure password scheme.The other methods include biometric and graphical methods which have their own drawbacks. The graphical passwords use a click based authentication scheme. The persuasive cued click points method uses the concept of persuading the user to select the password. Here the prediction of password is difficult for the hackers as it is generated in a random manner.

1.1. Graphical Passwords

Graphical passwords provide an alternative to text-based passwords that is intended to be more memorable and usable because graphical passwords rely on our ability to more accurately remember images than text [2].In the click-based password m ethod we use a concept called as PassPoints [3,4]which consists of sequence of click points on a given image.The selection of locations or pixels in the image will be based only on the particular sequence. When the location or pixel in the first image is given correctly, then the next image will be displayed to the user in a particular sequence. The user will have to select the correct location or pixel in the sequence of images that will be displayed consequently.

The problem that frequently occurred while using the concept of cued click points concept is that, the user will have to select the location or pixel in the given image which will be the same order for the login process. The other classification of the password scheme that is used in the graphical password scheme is pass points. The difference between cued click points concept and the pass points is that in password scheme using pass points the user have to select some specific location or pixel in a

particular image. This method proved to be less secure as there are many possibilities to trace the locations or pixels in a single image.

1.2. Biometric Passwords

To overcome the difficulties of the graphical password scheme biometric password method came into existence. The biometric system offers several advantages. They are more reliable than the password - based authentication system as the biometric passwords cannot be forgotten or be lost. They are also difficult to copy and to be distributed. They also require the person to be authenticated should be present at the time of authentication. So it is difficult to forge the identification of the person or user. Some of the different biometric methods used are

1. Face recognition
2. Fingerprint
3. Hand Geometry
4. Iris scan
5. Keystroke
6. Signature
7. Voice

Though the biometric methods offer different methods for authentication and have advantages over click points and pass points concepts, the biometric password system also has its own drawbacks. For example, if due to some unforeseen accidents if the fingers or face get damaged, then the biometric system using face recognition and finger print impression will get failed. The similar method is applicable for rest of the biometric concepts too. To overcome the difficulty of using the biometric method, we use the concept of persuasive cued click points.

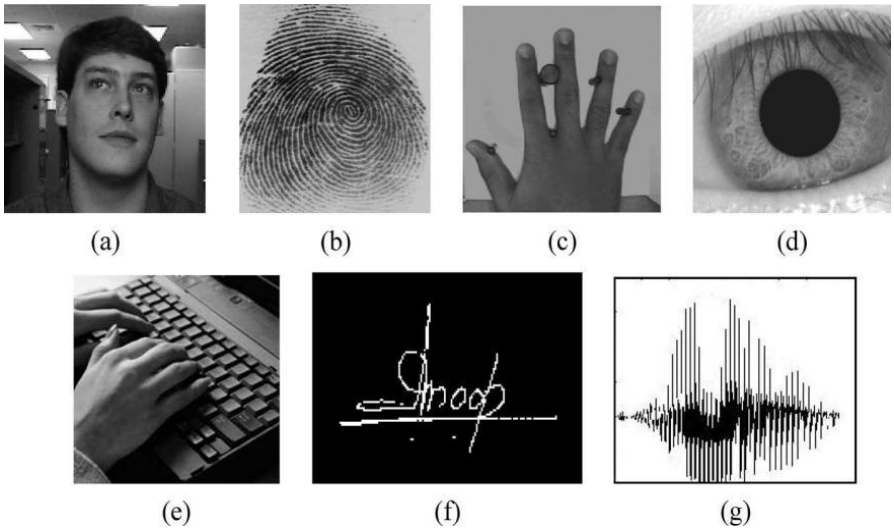

Fig1. *Examples of the different biometric methods*

2. PERSUASIVE CUED CLICK POINTS (PCCP)

The persuasive technology was first proposed by Fogg as a technology to make the users to have a better authentication system. The authentication system using the persuasive technology will allow users to select stronger passwords.

A precursor to PCCP, Cued Click-Points (CCP) was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Rather than five click-points on one image, CCP uses one click point on five different images shown in sequence. The next image displayed is based on the location of the previously entered click-point, creating a path through an image set.

Users select their images only to the extent that their click-point determines the next image.

Creating a new password with different click-points results in a different image sequence. The authentication method using the persuasive click points uses a more secure scheme for passwords. In

this method we have to select a location or pixel in the given image. When the pixel value is given correctly then the next image will be opened in a sequence. The pixel value will be generated in a random manner. So it is difficult for the hackers to find the pixel value which will be generated in a random manner.

The random order in which the pixel value should be given will be known only to the user. This is made possible by a simple technique. The images that are used for the password will be stored in a database. The random number in which the pixel value is to be given by the user will be intimated to the user through his mail or through his mobile phone.

In case if the hacker finds the first image by brute force attack, it will be difficult for the hackers to find the second pixel value as the pixel value will be generated randomly. The other advantage of this method is, if the pixel value entered proves to be wrong, then the next image will be displayed even in such cases. But the secure way that lies here is that only if the correct value is given, the user will be able to login. If the wrong pixel value is entered, next image will be displayed which not lead to the correct login will screen. The other advantage is that, only the user will know the random order of the pixel value generated. This is because the random order will be sent to user's mobile or to the mail id of the user.

3. METHODOLOGY

This system uses the concept of PCCP which provides high security .PCCP uses the persuasive technology which was introduced by Fogg encourages the user to select stronger passwords. It makes user to select password in a more secured way. Sequence of images will be presented to the user. The click points which the user should select for the correct login will be generated to the user in a random manner. The user should select one click point per image. Based on the click point chosen next image will be displayed. To login they should use the correct sequence of click points. This system will be difficult for attackers where the sequence of image cannot be predicted easily. This method does not provide any alert messages, if the chosen image is wrong. It will be known to them only during the final click point. So the chance of guessing the sequence is very low.

At first, registration of image will be done. There is a location called viewport in the image which will be positioned randomly anywhere in it. The user should select the appropriate point in the viewport for correct login, and they cannot be able to click anywhere outside the viewport. To reposition it shuffle button can be used. Shuffle button can be used only during creation of passwords. Later the image will be displayed normally without viewport to the user and they may click anywhere in the image. We apply this method of authentication in the bank sector. The modules used are described below.

4. MODULES DESCRIPTION

The modules used are listed as follows:

1. Authentication
2. Graphical passwords
3. Image Based Registration and Authentication System (IBRAS):
4. Admin Process

4.1. Authentication

Authentication is a function where a user presents some credentials to the system. If the system recognizes this set of credentials or the credentials match a given set on the system, then the user is said to be authorized otherwise the user is not authorized. The user needs to be authorized to request services from the system. Before a user can be authenticated to the system, he has to be registered with the system for the first time. This step is called registration. So, for a new user, he has to get registered with a system and then authenticated before he can request services. In a basic authentication process, a user presents some credentials like user ID and some more information to prove that the user is the true owner of the user ID.

This process is simple and easy to implement. An example of this type of authentication process is the use of user ID and password. A complicated process involves a user ID, password and a key value

generated with time and which changes constantly at fixed intervals. A user is authenticated only if all three values are right. This is better and more secure than the basic authentication process as the user has to be there physically to use the changing key. Our authentication system can be classified under the simple authentication process which is more secure and powerful than the password based system.

4.2. Graphical Passwords

This is a simple system where a user presents a user ID and a password to the system. If the user ID and password match with the one stored on the system, then the user is authenticated. More details about the graphical passwords have been already discussed above.

4.3. Image Based Registration and Authentication System (IBRAS)

IBRAS is a simple authentication system, which uses images as passwords. The user submits user ID and an image as credentials to the system. If the image matches with the one stored in the system, the user is authenticated. Images are easy to remember. It is not easy to guess images. Performing brute force attacks on such systems is very difficult. A first time user has to register him with the system by providing all his details. The interface guides the user in a step-by step fashion. No major change is to be made to the existing password based Systems to incorporate the use of images.

The system remains simple as the Password based one. The images are not stored in the system. Only the hashed values are stored. The user carries the image with him. This system is easy for Internet applications also.

4.4. Admin Process

We take the banking application as an example to explain the admin process. The process is explained as follows:

4.4.1. Account Creation

Create account in user Send User

Details Mail & Message

4.4.2. Reports

Customer Details Deposit Details

Checking all customer Transactions

4.4.3. User View (encryption Format)

Click Point

Mail ID

Secret questions and answers

5. SYSTEM ARCHITECTURE

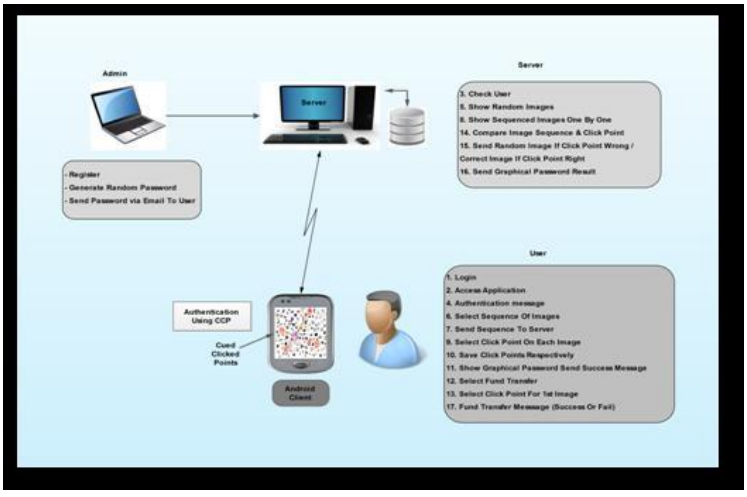

Fig2. *Architecture of M-Banking System*

4.5. Algorithm Analysis for M-Banking System

The algorithm used for M-Banking is SHA1. SHA1 stands for "Secure Hashing Algorithm". It is a hashing algorithm designed by the United States National Security Agency and published by NIST. It is the improvement upon the original SHA0 and was first published in 1995. SHA1 is currently the most widely used SHA hash function, although it will soon be replaced by the newer and potentially more secure SHA2 family of hashing functions. It is currently used in a wide variety of applications, including TLS, SSL, SSH and PGP.

SHA1 outputs a 160bit digest of any sized file or input. In construction it is similar to the previous MD4 and MD5 hash functions, in fact sharing some of the initial hash values. It uses a 512 bit block size and has a maximum message size of 2^4 1 bits.

Check No. of Satellites Visible = n If (N>3) then get the lat and long It checks this condition 3 times for getting confirms lock. So the time complexity of this algorithm is O(n^3). The space complexity of this project depends on the data client wants to store in database. More the duration of data more is the space complexity.

4.6. SHA1 Algorithm Description

1. Padding
    - Pad the message with a single one followed by zeroes until the final block has 448 bits.
    - Append the size of the original message as an unsigned64 bit integer.
2. Initialize the 5 hash blocks (h0, h1, h2, h3, h4) to the specific constants defined in the SHA1 standard.
3. Hash (for each 512bit Block)
    - Allocate an 80 word array for the message schedule
        - Set the first 16 words to be the 512bit block split into 16 words.
        - The rest of the words are generated using the following algorithm ∫ word [i3] XOR word [i8] XOR word [i14] XOR word [i16] then rotated 1 bit to the left.
    - Loop 80 times doing the following. (Shown in Image1)
        - Calculate SHAfunction () and the constant K (these are based on the current round number.
        - e=d
        - d=c
        - c=b (rotated left 30)
        - a = a (rotated left 5) + SHAfunction () + e + k + word[i]
    - Add a, b, c, d and e to the hash output.
4. Output the concatenation (h0, h1, h2, h3, h4) which is the message digest

6. CONCLUSION

The common security goal in password-based authentication systems is to increase the effective password space. This is achieved using user choice and is implemented using Persuasive Cued Click Points. This technique is highly suitable for places where high level security is required. A key feature in PCCP is that creating a harder to guess password is the path of least resistance and is achieved in this method, likely making it more effective than schemes where secure behaviour adds an extra burden on users. The approach has proven effective at reducing the formation of hotspots and patterns, thus increasing the effective password space, while maintaining usability.

ACKNOWLEDGEMENT

We would like to thank Prof. Jyoti Raghatawan for their guidelines in writing this paper.

REFERENCES

[1] A. Adams and M. Sasse. Users are not the enemy. Communication of the ACM, 42(12):41– 46, 1999.

[2] Nelson, D.L., Reed, U.S., and Walling, J.R. PictorialSuperiority Effect. Journal of Experimental Psychology:Human Learning and Memory 2(5), 523-528, 1976.

[3] Wiedenbeck, S., Birget, J.C., Brodskiy, A. and Memon, N.Authentication Using Graphical Passwords: Effects ofTolerance and Image Choice. Symp. on Usable Privacy and Security (SOUPS) 2005.

[4] S. Chiasson , P. C. van Oorschot, and R. Biddle. A usability study and critique of two password managers. In 15th USENIX Security Symposium, August 2006.

[5] S. Gaw and E. Felten. Password management strategies for online accounts. In 2nd Symposium On Usable Privacy and Security (SOUPS), July 2006.

[6] A. Dirik , N. Menon, and J. Birget. Modeling user choice in the Passpoints graphical password scheme. In 3rd ACM Conference on Symposium on Usable Privacy and Security (SOUPS), July 2007.

AUTHORS' BIOGRAPHY

Supriya Ghadge is a Student of Computer Engineering and Pursuing Bachelor of Engineering in RMDSSOE, Pune, India

Snehal Kate is a Student of Computer Engineering and Persuing Bachelor of Engineering in RMDSSOE, Pune, India

Vaibhav Mohite is a Student of Computer Engineering and Persuing Bachelor of Engineering in RMDSSOE, Pune, India

Shweta Patil is a Student of Computer Engineering and Persuing Bachelor of Engineering in RMDSSOE, Pune, India