International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471
Vol. 2 Issue 4, April-2013, pp: (10-15), Available online at: www.erpublications.com

M-Banking using Steganography and Cued Click Points

Ms.Vaishali Baviskar[1], Mayur Sanpurkar[2], Amit Patel[3], Makarand Jadhav[4], Gaurav Modi[5]
Department of Computer Science
G. H. Raisoni Institute of Engineering and Technology, Pune, India

Abstract: Recently, with the awareness of businessmen and consumers and the development of mobile technologies, the potential use of mobile devices in financial applications such as banking and stock trading has seen a rapid increase. However, the security challenges being faced are diverse and increasing in number because of huge amount of money flowing across the mobiles. There have been several attempts in the field to preserve anonymity of user and protect them from several attacks but due to many security flaws these schemes are not feasible for real-life implementation. In this paper we focus on mobile banking and provide a scheme based on Cued Click Points authentication for a user. We also propose the use of steganography as a means to improve the communication channel for any intrusion by the hackers.

Keywords: Authentication, graphical passwords, guessing attacks, computer security.

1. INTRODUCTION

There has been a great deal of hype for graphical passwords since two decade due to the fact that primitive's methods suffered from an innumerable number of attacks which could be imposed easily. Here we will progress down the taxonomy of authentication methods. To start with we focus on the most common computer authentication method that makes use of text Passwords. Despite the vulnerabilities, it's the user natural tendency of the users that they will always prefer to go for short passwords for ease of remembrance [9] and also lack of awareness about how attackers tend to attacks. Unfortunately, these passwords are broken mercilessly by intruders by several simple means such as masquerading, Eaves dropping and other rude means say dictionary attacks, shoulder surfing attacks, social engineering attacks [9][1]. To mitigate the problems with traditional methods, advanced methods have been proposed using graphical as passwords .The idea of graphical passwords first described by Greg Blonder (1996). For Blonder, graphical passwords have a predetermined image that the sequence and the tap regions selected are interpreted as the graphical password. Since then, many other graphical password schemes have been proposed. The desirable quality associated with graphical passwords is that psychologically humans can remember graphical far better than text and hence is the best alternative being proposed. There is a rapid and growing interest in graphical passwords for they are more or infinite in numbers thus providing more resistance. The major goal of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess. The following Figure 1 is the depiction of current authentication methods Biometric based authentication systems techniques are proved to be expensive, slow and unreliable and hence not preferred by many. Token based authentication system is high security and usability and Accessibility compare then others. But this system employ knowledge based techniques to enhance security. But the current knowledge based techniques are still immature. For instance, ATM cards always go hand in hand with PIN number.

2. TAXONOMY OF AUTHENTICATION

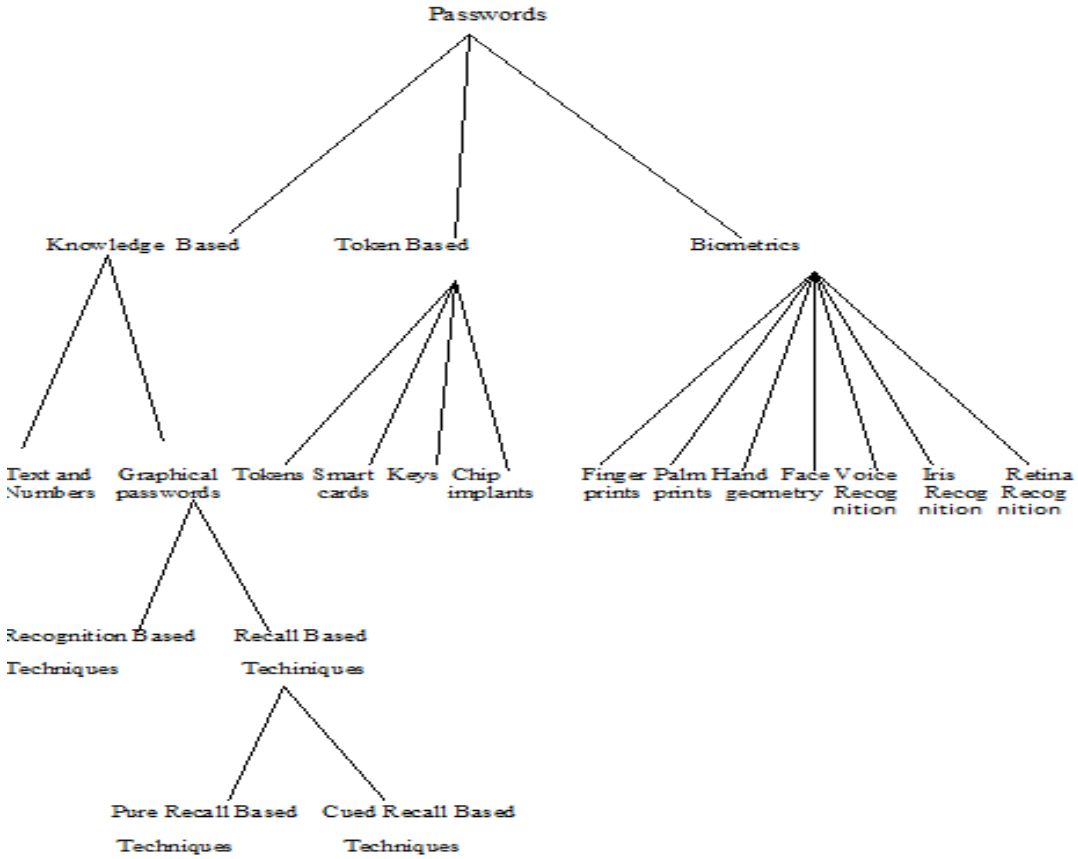

Figure 1: Taxonomy of Password Authentication Techniques

So the knowledge based techniques are the most wanted techniques to improve real high security. Recognition based & recalls based are the two names by which graphical techniques could be classified.

3. BACKGROUND ON GRAPHICAL PASSWORD SYSTEMS

Graphical passwords were first described by Blonder. Since then, many other graphical password schemes have been proposed. Graphical password systems can be classified as either recognition-based (image based scheme, cued recall-based (image based scheme) or pure recall-based (grid based
scheme.

3.1 Steganography

Steganography is an of art hiding secret messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The message is altered in a way to disguise the secret message in images, videos etc. In our scheme also we use steganography to hide login information before transmitting. The hiding technique used must have sufficiently high capacity and must be robust.

3.2 Recall based techniques:

In this section we discuss recent there types of click based graphical password techniques:
1. Pass Points (PP)
2. Cued Click Points (CCP)
3. Persuasive Cued Click- Points (PCCP)

3.2.1 Pass point (PP)

Based on Blonder's original idea [2], Pass Points (PP) [2] is a click-based graphical password system where a password consists of an ordered sequence of five click-points on a pixel-based image as shown inFigure.1 To log in, a user must click

within some system-defined tolerance region for each click-point. The image acts as a cue to help users remember their password click-points

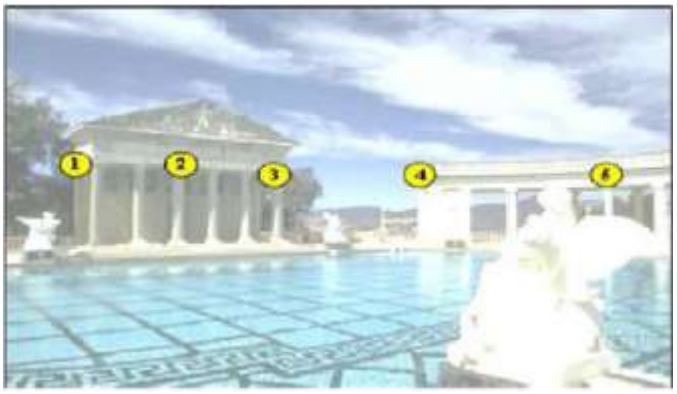

Figure 2: Pass Point

3.2.2 Cued Click Points (CCP)

CCP [1] was developed as an alternative click based graphical password scheme where users select one point per image for five images Figure.3: The interface displays only one image at a time; the image is replaced by the next image as soon as a user selects a click point. The system determines the next image to display based on the user's click-point on the current Image. The next image displayed to users is based on a deterministic function of the point which is currently selected. It now presents a one to-one cued recall scenario where each
Image triggers the user's memory of the one click-point on that image. Secondly, if a user enters an incorrect click-point during login, the next image displayed will also be incorrect. Legitimate users who see an unrecognized image know that they made an error with their previous click-point. Conversely, this implicit feedback is not helpful to an attacker who does not know the expected sequence of images.

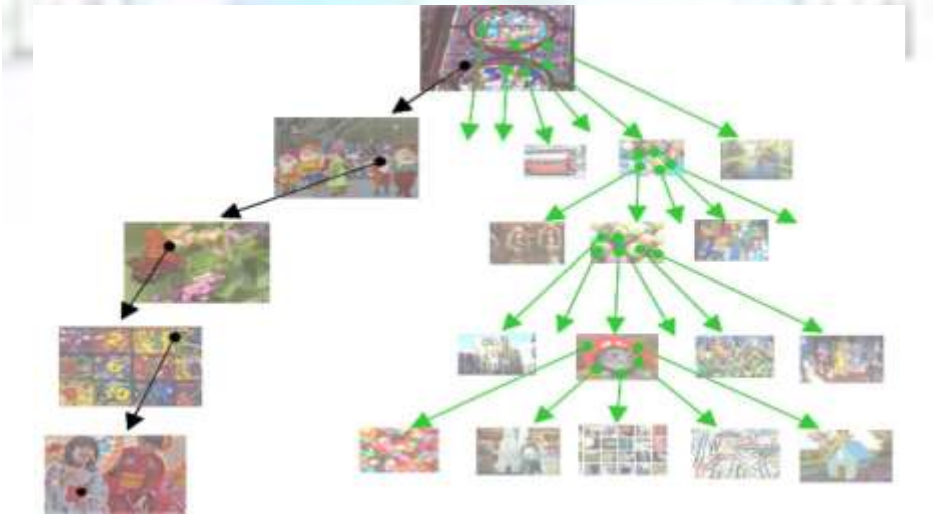

Figure 3: Cued Click Points

3.2.3 Persuasive Cued Click- Points (PCCP)

To address the issue of hotspots, PCCP was proposed [2]. As with CCP, a password consists of five click points, one on each of five images. During password creation, most of the image is dimmed except for a small view port area that is randomly positioned on the image as shown in Figure. 4. Users must select a click-point within the view port. If they are unable or unwilling to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots. A user who is determined to reach a certain click-point may still shuffle until the view port moves to the specific location, but this is a time consuming and more tedious process.

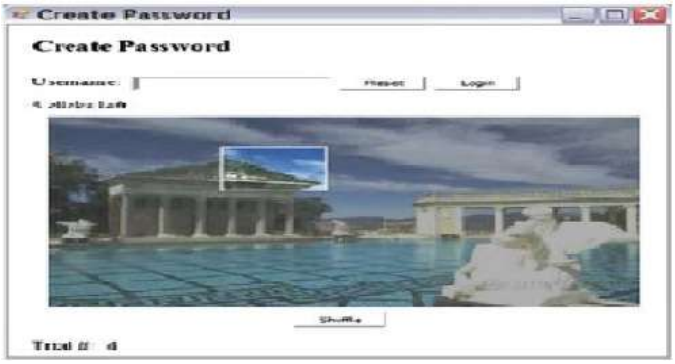

Figure 4: the PCCP password creation interface

4. DISCUSSION

"Will Graphical passwords circumvent?
Text based passwords?"

Here we briefly exam some of the possible techniques for breaking graphical passwords and try to do a comparison with text based passwords.

Dictionary attacks

Since recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. For some recall based graphical passwords [10], it is possible to use a dictionary attack but an automated dictionary attack will be much more complex than a text based dictionary attack. More research is needed in this area Overall; we believe graphical passwords are less vulnerable to dictionary attacks than text-based passwords.

Guessing

Unfortunately, it seems that graphical passwords are often predictable, a serious problem typically associated with text-based passwords. More research efforts are needed to understand the nature of graphical passwords created by real world users.

Shoulder Surfing

Like text based passwords, most of the graphical passwords are vulnerable to shoulder surfing. At this point, only a few recognition based techniques are designed to resist shoulder-surfing.

Spy ware

Except for a few exceptions, key logging or key listening spy ware cannot be used to break graphical passwords. It is not clear whether "mouse tracking" spy ware will be an effective tool against graphical passwords. However, mouse motion alone is not enough to break graphical passwords. Such information has to be correlated with application information, such as window position and size, as well as timing information.

Social engineering

Comparing to text based password, it is less convenient for a user to give away graphical passwords to another person. For example, it is very difficult to give away graphical passwords over the phone. Setting up a phasing web site to obtain Graphical passwords would be more time consuming.

5. PROPOSED SYSTEM

Now-a-days, all business, government, and academic organizations are investing a lot of money, time and computer memory for the security of information. Online password guessing attacks have been known since the early days of the Internet, there is little academic literature on prevention techniques. This project proposes a click-based graphical password system. The aim of this work is to provide 2 levels in terms of security for transaction in banking applications. First we are making use of

Steganography for sending user id and password on server using Steganography encoded image from the user's mobile phone , Once the user is authenticated he will be shown with a graphical password screen. As with CCP User is shown with sequence of images with 4x4 blocks; user has to select one block from each image. Secondly, if a user enters an incorrect click-point during login, the next image displayed will also be incorrect. Legitimate users who see an unrecognized image know that they made an error with their previous click point. Conversely, this implicit feedback is not helpful to an attacker who does not know the expected sequence of images. This way we would improve security by using "Steganography" technique and graphical authentication in mobile banking applications. Upon development of m-commerce as one of the new branches of e-commerce, m-banking has emerged as one of the main divisions of m-commerce. As the m-banking was received very well, it has embarked upon supply of various services based on different systems and with the aid of various services such as the short messaging service (SMS). However, in spite of its advantages, m-banking is facing some challenges as well. One of these challenges is the issue of security of this system. This project presents a method for increasing security of the information requested by users with the use of Steganography method. In this method, instead of direct sending of the information, it is encrypted and hidden in a picture using random bit Steganography technique. Then the picture is sent to the server. After receiving the picture on server, the sample http download socket program downloads the image, decrypts it and decodes to receive the message. The message is then processed on the server to verify user credentials such as user name and password. In this project the total number of login attempts from unknown hosts are limited, legitimate users in most cases (e.g., when attempts are made from known, frequently-used machines) can make several failed login attempts.

5.1 Architecture

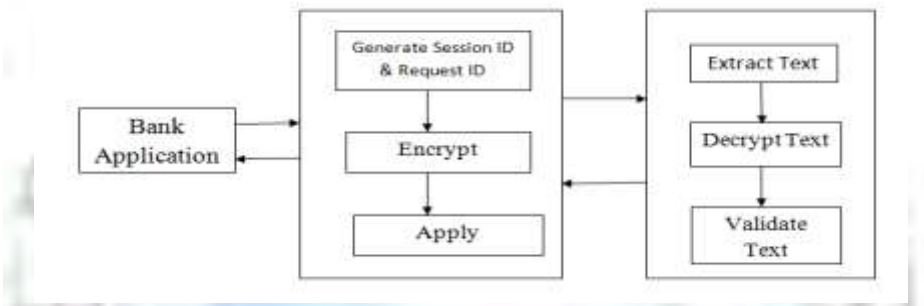

Figure 5: Architecture

6. CONCLUSION AND FUTURE WORK

In this paper, we have presented weaknesses of some of the previous remote user authentication schemes. Firstly, we showed that how the previous schemes were vulnerable to insider attack and did not preserve anonymity of a user, long and random password for a user to remember, no provision for revocation of lost or stolen smart card and no support for session key agreement during authentication process. To overcome the identified problems we proposed an enhanced steganographic approach which improves all the identified weaknesses and is more secure and robust for real-life use. The proposed scheme can withstand the forged authenticating attacks besides providing better communication with the system as the information traveling across the insecure channel is always hidden. The system is very secure as mutual authentication takes place between the communicating parties for processing of the supplied information. Moreover, our scheme is robust, practical and more efficient than other schemes.

In future, more practice handling and using such schemes especially the biometrics within the experimental setting might provide more realistic data, reducing the potential strain and bias of first-time use. Practical implementation of the same is also required to have a real life environment for more developments to take place. Use of biometrics may certainly lead to real life physical authentication systems. More robust techniques for face and voice recognition need to be explored.

REFERENCES

[1]. Chippy.T R.Nagendran "Defenses Against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points" International Journal of Communications and Engineering Volume 03– No.3, Issue: 01 March2012 .

[2]. Sonia Chiasson, Member, IEEE, Elizabeth Stobert, Student Member, IEEE, Alain Forget,Robert Biddle, Member, IEEE, and Paul C. van Oorschot, Member, IEEE, "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism." IEEE transactions on dependable and secure computing, vol. 9, no. 2, March/April 2012.

[3]. S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwes Instruction and Computing Symposium, 2004.

[4]. http://en.wikipedia.org/wiki/Steganography.
[5]. Prof. Akhil Khare, "Efficient Algorithm for Digital Image Steganography".
[6]. L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, an Electronic Bulletin for Undergraduate Research, vol. 4, 2002.
[7]. I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.
[8]. S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003.
[9]. A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42, pp. 41-46, 1999.
[10]. I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.
[11]. Alain Forget, Sonia Chiasson, and Robert Biddle,"Shoulder-Surfing Resistance with Eye- Gaze Entry in Cued-Recall Graphical Passwords", ACM 978- 1-60558-929-9/10/04, April 10 – 15, 2010.
[12]. Jessica Fridrich, "Steganography in digital media".
[13]. Dushyant Goyal and Shiuh-Jeng Wang, "Steganographic Authentications in conjunction with Face and Voice Recognition for Mobile Systems".