Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

A Survey of Password Based Techniques in Cyber Security

[1]Aswini and [2]Kavya,
[1]Assistant Professor, [2]Research Scholar
[1, 2]Department of computer science, St. Joseph's College of Arts and Science for Women, Hosur, Tamilnadu, India

***Abstract*--**Core banking is a set of services provided by a group of networked bank branches. Bank customers may access their funds and perform other simple transactions from any of the member branch offices. The major issue in core banking is the authenticity of the customer. Due to unavoidable hacking of the databases on the internet, it is always quite difficult to trust the information on the internet. To solve this Problem of authentication, the proposed system is based on click based graphical password system that not only guides and helps the user for password selection but also encourages the user to select more random distributed password.

Keywords *-- Two-factor Authentication, Graphical Password, OTP.*

I. INTRODUCTION

User authentication is a fundamental component in most computer security contexts. It provides the basis for access control and user accountability. While there are various types of user authentication systems, alphanumerical username/passwords are the most common type of user authentication. The major issue in core banking is the authenticity of the customer. Due to unavoidable hacking of the databases on the internet, it is always quite difficult to trust the information on the internet. To solve this Problem of authentication, we are proposing an algorithm based on image processing, improved steganography which is visual cryptography.

The problem of Knowledge based authentication mechanism (KBAM) typically text based password are well known. The goal of an authentication system is to support users in selecting the superior password. An alternative to alphanumeric password is the graphical password. Graphical password uses images or representation of an image as a password. Human brains easily recognize pictures than the text. Most of the time user create memorable password which is easy to guess but strong system assigned password are difficult to remember. An authorization system should allow user choice while influencing user towards stronger passwords.

II. PASSWORD CATEGORIES

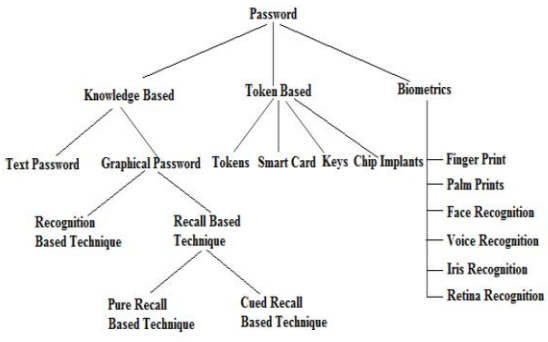

Figure 1: Categories of Password

Figure.1 is the representation of current authentication methods.

The problem with text based password is that user creates memorable password which can be break easily and also the text password has limited length password which means that password space is small. Biometric based authentication techniques are somewhat expensive, slow and unreliable and thus not preferred . Token based authentication system has high security and usability and accessibility then the others. Also the system uses the knowledge based techniques to enhance the security of token based system. But the problem with token based system is that if token get lost, the security get also lost.

Therefore the Knowledge based authentication techniques are most preferable technique to improve the real high security. Graphical Password is one of the knowledge based technique and it is categorized into Recognition based and Recall based. In Recognition based techniques user has to recognize or reproduce the things during the login where as in case of recall based technique user has to recall the things during the login in such a way that whatever they selected during the password creation they have to recall it in the same manner.

III. METHODS & DRAWBACKS IN EXISTING SYSTEM

A. Movable Frame Algorithm

The moveable frame algorithm proposed in 2002 had a similar idea to that of triangle method. However in its case the user had to select three objects from K objects in the login phase. As it is shown in Fig. 2.1, only 3 pass objects are displayed at any given time and only one of them is placed in a movable frame.

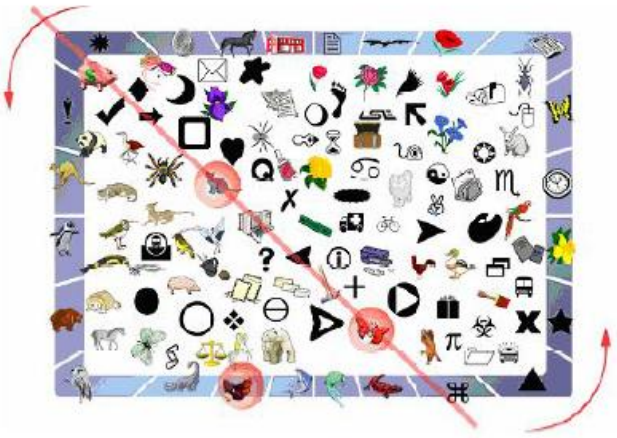

Figure 2.1: A Sample Of Movable Frame Algorithm

The user must move the frame until the three objects line up one after the other. These operations minimize the random movements involved in finding the password .

Drawbacks:

Just like in the triangle algorithm, there are many objects involved in this algorithm which can lead to the user being unsatisfied and in most cases will confuse users.

B. Picture Password Algorithm

This algorithm was designed especially for handheld devices like Personal Digital Assistant (PDA) in 2003. According to Figure 2.2 during enrollment, the user selecting a theme identifying the thumbnail photos to be applied and then registers a sequence of thumbnail images that are used as a future password. If the device is powered on, then the user must input the true sequence of images but after successful log-in the user can change the password.

In this algorithm the password space will be small because the number of photos is limited to 30. In order to solve this problem, the designer added a second step to the algorithm. This means the user can select two thumbnails together to compose the new alphabet element by using a shift key to select uppercase or special characters.

Figure 2.2 A Sample Of Picture Password Algorithm

Drawbacks:

The memorability will be more complex when the second part which solves the password space's problem is added to the algorithm.

IV. STORY ALGORITHM

The Story Algorithm that was proposed in 2004, categorized the available pictures into nine categories namely animals, cars, women, foods, children, men, objects, natures and sports. This algorithm was proposed by Carnegie Mellon University to be used for different purposes. In this method the user selects the password from the mixed pictures in the nine categories in order to make a story.

V. BLONDER'S SCHEME

Graphical Password is one of the knowledge based technique and it is categorized into Recognition based and Recall based. In Recognition based techniques user has to recognize or reproduce the things during the login where as in case of recall based technique user has to recall the things during the login in such a way that whatever they selected during the password creation they have to recall it in the same manner.

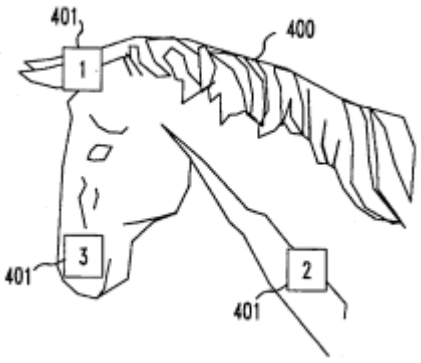

Figure 2.3 Graphical Password Scheme Sample

Graphical password scheme in which user click on several different predefined locations on a predetermined image. During login, the user has to click on the approximate area of those locations represented in Fig.2.3. Basically the image helps the user to summon up their passwords and therefore this scheme is considered more suitable than unassisted recall. The problem with this system is that boundaries are predefined which results various attacks are easily possible.

VI. PASS-POINT SCHEME

Figure 2.4 Passpoint Graphical Password Scheme Sample

Pass-point graphical password scheme: In which password consists of a sequence of 5 different click points on a given image represent in Fig.2.4. During password creation user can select any pixel in the image as a click-points and during authentication the user has to repeat the same sequence of clicks in correct order within a system defined tolerance square of original click-points. Pass-point used the robust discretization technique.

The problem with this scheme is that HOTSPOT: (area of an image where user more likely to select the click-point) and

also user makes certain kinds of patterns in order to remember the password which means pattern formation attacks are easily.

VII. PROPOSED SYSTEM

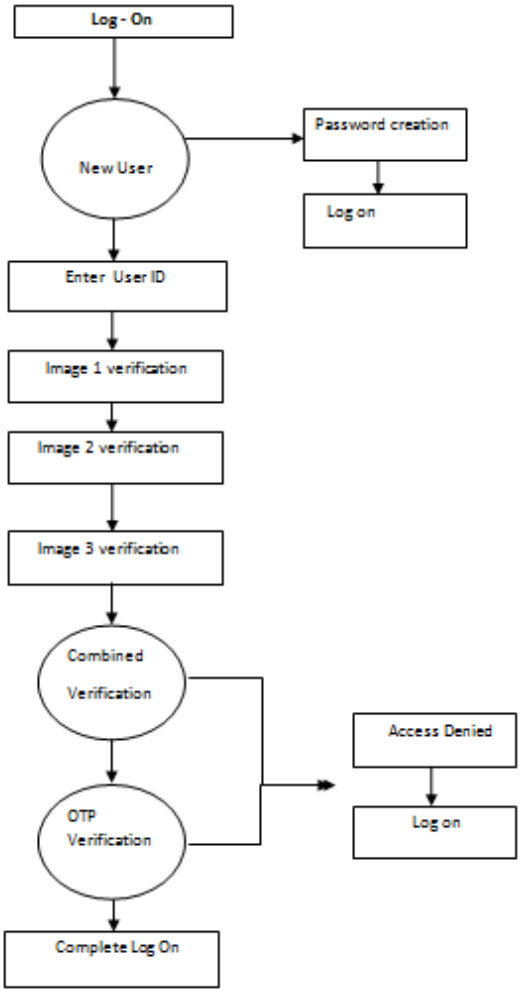

Figure 3.1 System Architecture of Proposed System

In the net banking system, the password of customer may be hacked and misused. Thus security is still a challenge in these applications. Here we propose a technique to secure the customer information and to prevent the possible forgery of password hacking and its system represent in Figure.3.1.The proposed system is based on two-factor authentication technique one is OTP other one is click based graphical password system that not only guides and helps the user for password selection but also encourages the user to select more random distributed password.

The proposed system is based on Persuasive Technology which motivates and influence people to behave in a desired manner. The proposed system combines the Persuasive features with the cued click point to make authentication system more secure. Basically during password creation the part of an image which is less guessable is highlighted and user has to select the click-point within the highlighted portion and if the user is unable to select the click-point then he can move towards the next highlighted portion by pressing the shuffle button. The highlighted part of an image basically guides users to select more random passwords that are less likely to include hotspots. Therefore this works encouraging users to select more random, and difficult passwords to guess. During Login, images are displayed normally and user has to select the click point as chosen at the time of password creation but this time highlighted portion is not present as it only provides the system suggestion. An important usability goal of proposed system is to support users in selecting password of higher security with larger password space. The proposed system removes the pattern formation attack and Hotspot attack (it is an area of an image where most of the user is selecting it as the click-point).Also it removes the shoulder surfing attack. Cued click -point which was intended to reduce the HOTSPOT and pattern formation attack. CCP uses one click point on five different images instead of five click-points on one image. The next image to be displayed is based on previous click-point and the user specific random value by using a deterministic function.

Here the password entry becomes a true cued recall scenario wherein each image triggers the memory of corresponding click-point.

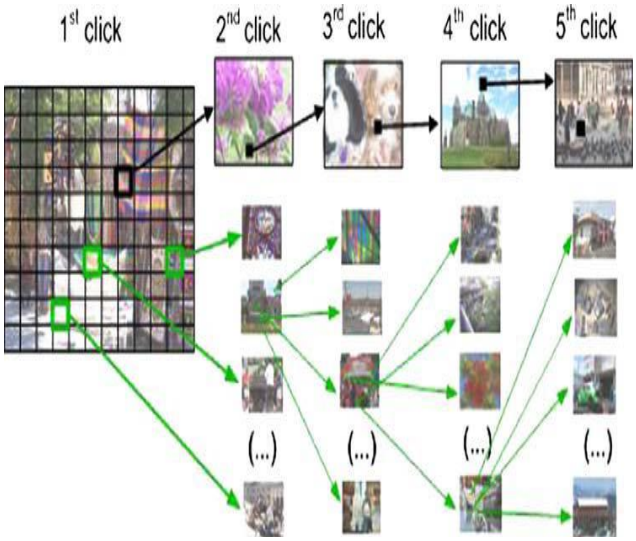

Figure 3.2 Click Points

VIII. ARCHITECTURE OF PROPOSED METHODOLGY

For legitimate users it provides implicit feedback such that while logging if user unable to recognize the image then it automatically alters the user that their previous click point is incorrect and user can restart the password entry whereas explicit indication is provided after the final click point. CCP also used the robust discretization technique. The problem with this technique is false accepted and false reject is possible

IX. OTP VERIFICATION

After the graphical password verification user can receive the OTP to user's registered mobile number as GUI password. After otp verification only the account holder can able to login to the account. The OTP sms will send through the sms gateway illustrated in Figure.3.3.

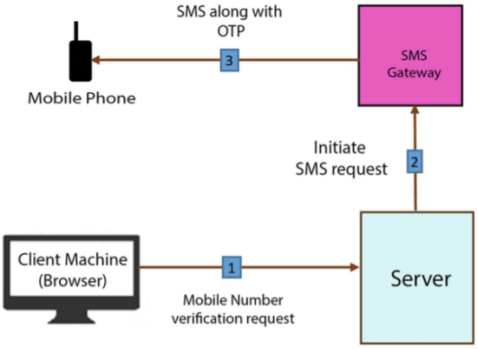

Figure 3.3 OTP from browser to mobile phone

The algorithm is:

HOTP(K,C) = Truncate(HMAC-SHA-1(K,C))

K	Shared key between client and server
C	8-byte counter value syncronized between client and server
Truncate()	Perform a dynamic truncation and reduction of the string to extract a 4-byte dynamic binary code. The result must extract minimum a 6-digit code, but also 7 and 8-digit code

Let:

K be a secret key
C be a counter

HMAC(K, m) = SHA1(K ⊕ 0x5c5c… ‖ SHA1(K ⊕ 0x3636… ‖ m)), where m is a "message", ⊕ means XOR, and ‖ means concatenation
Truncate be a function that selects 4 bytes from the result of the HMAC in a defined manner.
Then HOTP(K, C) is mathematically defined by
HOTP(K, C) = Truncate(HMAC(K, C)) & 0x7FFFFFFF
The mask 0x7FFFFFFF sets the result's most significant bit to zero. This avoids problems if the result is interpreted as a signed number as some processors do.For HOTP to be useful for an individual to input to a system, the result must be converted into a HOTP value, a 6–8 digits number that is implementation dependent.
HOTP-Value = HOTP(K, C) mod 10d, where d is the desired number of digits

X. ADVANTAGES OF PROPOSED SYSTEM

- An important usability goal of proposed system is to support users in selecting password of higher security with larger password space.
- Proposed system removes the pattern formation attack and Hotspot attack (it is an area of an image where most of the user is selecting it as the click-point).
- Also it removes the shoulder surfing attack.

CONCLUSION

The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. In this paper, we have conducted a comprehensive survey of existing graphical password techniques. The current graphical password techniques can be classified into two categories: recognition-based and recall based techniques.

Although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument.

Our preliminary analysis suggests that it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spyware. However, since there is not yet wide deployment of graphical password systems, the vulnerabilities of graphical passwords are still not fully understood. A prototype of the proposed model was implemented on a web platform using Java.

Results showed that graphical authentication has a high usability and that it is likely to replace text-based authentication methods in the near future. And even as of today, we can see graphical passwords being used in Windows8 OS as an alternate to text password, and also in touch based handheld devices like android smartphones, we see pattern locking mechanisms which is nothing but graphical authentication**.**

ACKNOWLEDGEMENT

We First of all, we thank God for giving us the necessary wisdom to accomplish this project. We take great pleasure to please the honorary acknowledgement to all those who have helped us both internally and externally for our project. We wish to express my sincere thanks to Mrs. Dhina Suresh, M.Sc., M.Phil., Head of the Department, Department of Computer Science, and Rev. Dr.(Sr). I.Arockia Rani, Secretary & Principal of St.Joseph's College Of Arts & Science For Women, Hosur for the valuable advice and guidance with constant encouragement and continuous support to complete the project work.

References

[1] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray H*ill, NJ*, U. S. Patent, Ed. United States, 1996.

[2] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91, no.12, pp. 2019 2020, Dec. 2003.

[3] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The Memorability and Security of Passwords," Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, eds., ch. 7, pp. 129-142, O'Reilly Media, 2005.

[4] S. Wiedenbeck, J. Waters, J. BirgetA. Brodskiy, and N. Memon, "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System," Int'l J.Human-Computer Studies, vol. 63, nos. 1/2, pp. 102-127, 2005.

[5] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice," Proc. First Symp. Usable Privacy and Security (SOUPS), July 2005.

[6] A. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Trans. Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125-143, June 2006.

[7] Dirik, N. Menon, and J. Birget, "Modeling User Choice in the Passpoints Graphical Password Scheme," Proc. Third ACM Symp. Usable Privacy and Security (SOUPS), July 2007.

[8] Authentication Using Cued Click Points, Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007.

[9] Fogg, Persuasive Technologies: Using Computers to Change What We Think and Do. Morgan Kaufmann Publishers, 2010.