Hybrid Graphical Authentication Scheme Using Click Points and Personal Identification Number

Dr. M. Sulthan Ibrahim
Department of Computer Science
Assistant Professor and Head,Government Arts and Science College, Veerapandi-625534, Theni Dt, Tamil Nadu, India.

Abstract-*Last decade has witnessed a colossal evolution in terms of security especially allied to graphical password schemes. This paper work predominantly focuses to cater to the need of the people who strives hard to get their data secured completely and this necessity has imbued quite a lot of researchers to move forward to do some exploration related to graphical password of late. This paper's core aim is to develop a graphical password algorithm combining the features of click point techniques and personal identification number to ensure tradeoff between memorability & security. The experimental results showcased that the proposed approach is more secured and completely evades the shoulder surfing attacks.*

Keywords-Graphical passwords, Click points, Authentication

I. INTRODUCTION

Perched on a highly sophisticated technology oriented world, we the most intelligent species are at a vantage point. Today computer has become a part and parcel of human life and it helps the humans in every sphere of their life. With the ever increasing threats affecting the very security and privacy of the system, the need for a high security scheme or model is imperative. Most common method to secure a system is password. The password is the best form of authentication to gain access to a resource or a system. The password is not revealed from those not authorized to access, and those desires to acquire access are tested on whether they reveal the password to grant access to the system or resource. Today users interact with security technologies like password either inertly or lively. For inert use understandability may be adequate for users. For lively and active use people need ease of use, easy memory, efficiency, effectiveness and satisfaction.

The use of passwords dates back to ancient times and possesses a long history. Patrols guarding a location would challenge for a password or a secret word and they would allow the person in only if the password or the word is revealed. Today passwords are used to gain access to computer operating systems, mobile & smart phones, ATMs machines etc. Presently a password is used by the computer user for plethora of purposes namely logging in to computer accounts, logging on to email servers, accessing files/folders in a system, accessing databases, accessing networks, reading important contents in web sites.

Presently providing hi-tech user authentication is the most intricate task for the system developers. The well-known fact is that most computer systems and users employ knowledge-based authentication methods, such as text passwords and Personal Identification Numbers (PINs). The primary reason behind this is that they are simple to manage,understand and possess very little complexity in nature. In spite of these advantages the PIN and textual password has lot of snags and demerits. One of the main problems human's difficulty in remembering passwords.

Recent studies have revealed that users has the tendency to pick shorter passwords or passwords that are straightforward to remember such as vehicle number, first name, mobile number, date of birth etc. But the sad news is that these passwords can be easily guessed, broken and cracked. Since 1995 researchers has been constantly looking out for a new safe and secured authentication system that is easy to use as well as easy to remember. Recent studies proved that people perform far better when remembering pictures than textual words and the technique of graphical password came into existence.

The graphical password authentication scheme is not a new technology but it was introduced long back and various methodologies and techniques are implemented at various period of time.

II. RELATED WORKS

G. E. Blonder [1] is the pioneer of the graphical passwords. He introduced a technique that allow user to click with the aid of mouse on a few areas randomly on an image that is displayed on the screen. If all the selected spots are clicked rightly, the user will be authenticated and allowed to access the resources. G. E. Blonder's scheme was the first recall-based graphical password scheme which was under United States Patent.

DAS (Draw-a-secret)method is proposed by [8] Jermyn, Mayer, Monrose, Reiter and Rubin in 1999, which allows user to draw their unique password. A user is required to draw a simple picture on a grid using the mouse. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the user touches the same grids

in the same sequence, then the user is authenticated and allowed to gain an access.

Wiedenbeck [13] extended Blonder's idea by eliminating the predefined boundaries and allowing arbitrary images to be used [Wiedenbeck, S., 2005]. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of their chosen pixels and also in the correct sequence.

Chiasson et al.[15] proposed Cued Click-Points (CCP), a variation of Pass Points in which users click on one point per image for a sequence of images. The next image is displayed based on the location of the previous click-point, that is, each image after the first is a deterministic function of the current image and the coordinates of the user-entered click-point. If users click an incorrect point, a wrong image will be displayed.

The work of DeAngeli et al. [2] proposes that security of authentication methods can be judged in terms of three aspects namely guessability, observability, and recordability . Definitions of each are as follows,

Guessability: the minimum probability an assailant can guess the user's password (graphical and image) and breach the security level to obtain access to the resources illegally.

Observability: the minimum probability of an assailant being able to monitor the authentication proceedings and being able to reproduce the pattern or password to gain unauthorized access to the resources.

Recordability: the ease with which a user can record the user's password(graphical or otherwise) using modern day electronic gadgets with an intention to break into the security system without proper permission.

III. CHALLENGES IN GRAPHICAL PASSWORD

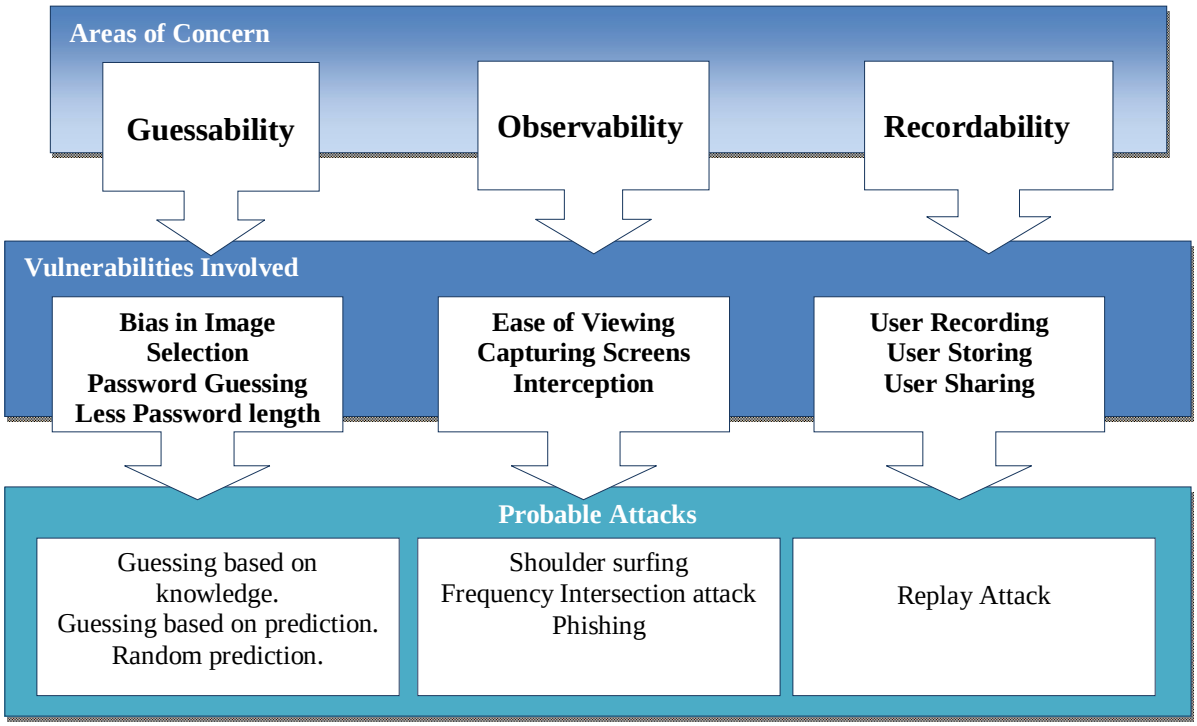

Figure 1: Threat model of graphical password

IV. PROBLEM STATEMENT

The foremost idea which triggered this work is lack of an excellent graphical password scheme available to provide utmost security. Users' inclination to handle alphanumeric passwords insecurely surfaces basically from long-term memory limitations. Most Users struggle remembering very complex, random passwords over time and also struggle to retain them but when the user provides easier password, it is easier to guess and breach.

Users normally cope up with password memory dilemma by declining the complications and number of passwords, but this reduces the very security of password. The attackers usually hack or use numerous methods to discover the graphical passwords. Usually, users pay no attention to such attacks, and use click point technique that are quite easy to unearth using shoulder surfing attacks.

V. EXISTING SYSTEM

The problems of knowledge-based authentication typically text-based passwords, are well known Users often create memorable passwords that are easy for attackers to guess, but strong system assigned passwords are difficult for users to remember. As far as graphical passwords are concerned, the user finds it difficult to remember the images clicked in sequence, and they suffer from various attacks.

VI. PROPOSED APPROACH

To overcome the snags like shoulder surfing and eavesdropping present in the graphical password authentication system, a new approach which combines the clicks with a personal identification number is proposed in this paper.

Click Point technique is a new graphical password scheme, wherein user selects one click point on each image rather than multiple click points on single image. During password creation, user has to select the images, sequence of the images and a click point for each image. This data is stored on a server which will be authenticating users as they enter graphical password. At the time of authentication, user has to select the correct click point on each of the images. Here the attacker has every possibility to secretly view the clicked images along with the sequence even though the images to be displayed during verification will be scrambled.

This paper introduces a hybrid approach, where the user decides a secret PIN for example “3526”. The user will have to click four images during registration since there are four digits in the pin. While clicking the user clicks the first image three times, second image five times, third image twice and the final image six times. The image clicked along with the sequence and the number of clicks clicked will be counted for each image will be stored in the server during registration.

The registration process is shown in the figure 2. This sample consists of 9 images where the user will click images with respect to his preferable PIN. The clicked image with sequence along with the PIN is stored in the database.

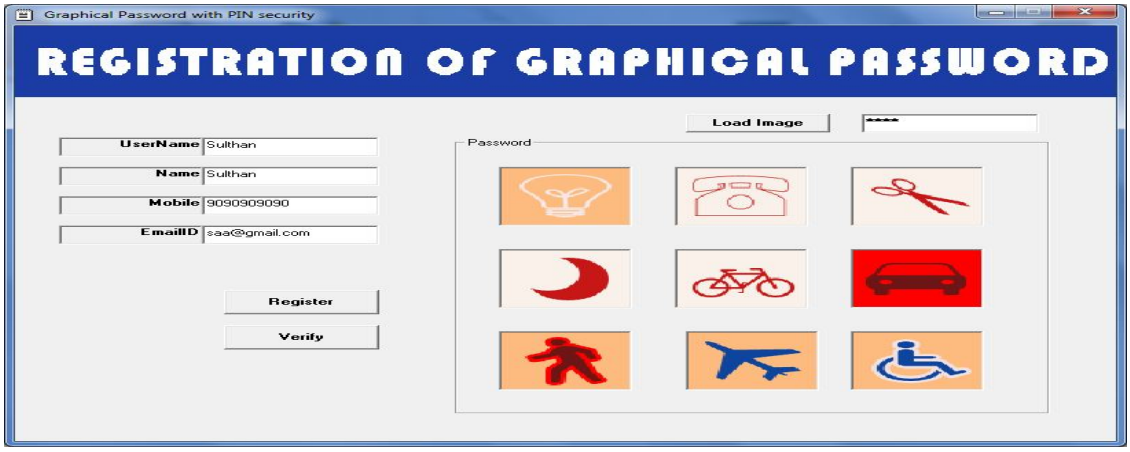

Figure 2: Registration process

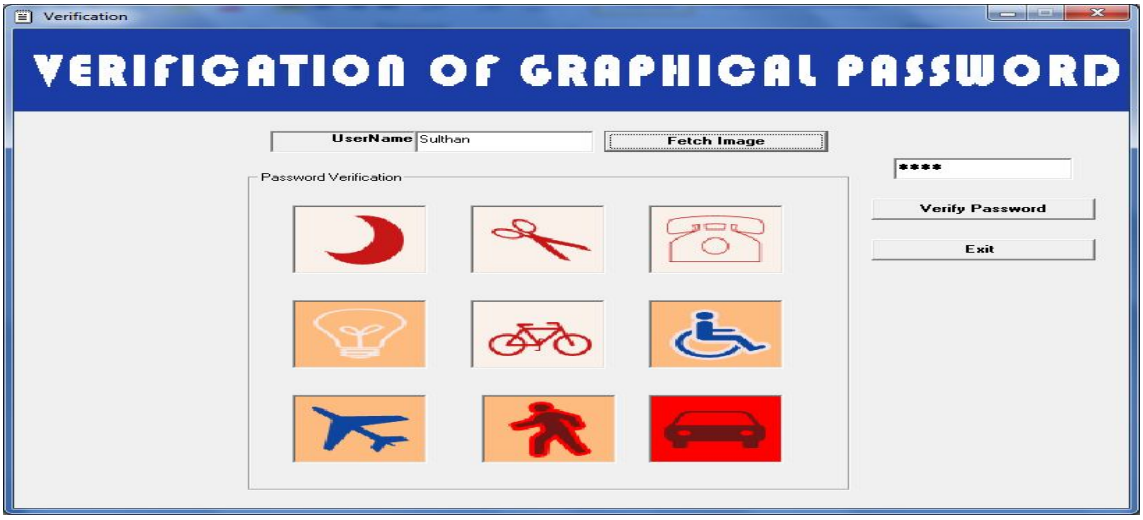

Figure 3: Verification Process

During verification phase the images displayed will be scrambled and displayed; the user will have to click the correct sequence of images with the registered number of clicks. If the sequence and the number of clicks matches with

that stored for a particular user in the database, the user will be allowed to proceed. The verification process is shown in figure 3.

VII. EXPERIMENTAL EVALUATIONS

The entire process is developed using C#.NET and SQL server in a machine with a configuration Intel core2 processor, 2 GB RAM and 2.25 GHz speed. The experimental results showcased that the graphical password is practically impossible to breach with the shoulder surfing attacks. The security levels of the proposed method are compared with the state of the art click point methods as shown in the table 1. From the results, it is quite clear that the proposed approach is far more secured.

Table 1: Comparison of various graphical schemes

Scheme	Passpoints	CCP	PCCP	Proposed
Login Time	10 – 40s	10-20s	12-75s	15 – 90s
Success Rate	40 – 85%	89%	85%	90%
memorability	Medium	Medium	Medium	High
Security	Low	Low	Medium	High

Table 1: Comparison of various graphical schemes

VIII.CONCLUSION

Better user interface design can influence users to select stronger passwords. A key feature of the proposed approach is that creating a harder to guess password is the path of-least-resistance, likely making it more effective than schemes where secure behavior adds an extra burden on users. The approach has proven effective at reducing the formation of hotspots and evading the shoulder surfing attacks. The primary goal of the proposed system was to increase the effective password security and creating a tradeoff between security and memorability.

REFERENCES

[1] G. Blonder, “Graphical Password”, InLucent Technologies, Inc., Murray Hill, NJ, United States Patent 5559961, 1996.
[2] Renaud K. and De Angeli A., “My Password is Here! An Investigation IntoVisuo-Spatial Authentication Mechanisms”, Interacting with Computers vol. 16 (6), pp. 1017-1041, 2004.
[3] 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, 1999, pp. 41-46.
[4] R. Dhamija and A. Perrig.“Déjà vu: A User Study Using Images for Authentication”, In Proceedings of the 9th USENIX Security Symposium, 2000.
[5] M. Kotadia, “Microsoft: Write down your passwords”, In ZDNet, Australia, 2005.
[6] R. Dhamija and A. Perrig. “Déjà vu: A User Study Using USENIX Security Symposium, 2000. Images for Authentication”, In Proceedings of the 9TH USENIX SECURITY SYMPOSIUM 2000.
[7] Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., Memon, N., “PassPoints: Design and Longitudinal Evaluation of a Graphical Password System”, International Journal of Human-Computer Studies, 63, 2005, pp. 102-127.
[8] I. Jermyn, A. Mayer, F. Monrose. M. K. Reiter and A. D. Rubin, “The Design and Analysis of Graphical Passwords”, InProceedings of the 8TH USENIX Security Symposium, 1999.
[9] Jansen, W., Gavrila, S., Korolev, V., Ayers, R., Swanstrom, R., “Picture Password: A Visual Login Technique for Mobile Devices”, NISTt NISTIR 7030, 2003.
[10] Sobrado, L and Birget, J. “Graphical Passwords,” The Rutgers Scholar , An Electronic Bulletin ofUndergraduate Research, Rutgers University, NewJersey, Vol. 4 (2002).
[11] D. Hong, S. Man, B. Hawes, and M. Mathews, “A password scheme strongly resistant to spyware”, In Proceedings of International conference on security and management, Las Vergas, NV, 2004.
[12] S. Brostoff and M. A. Sasse, “Are Passfaces more usable than passwords: A Field Trial Investigation”, In People and Computers XIV – Usability or Else: Proceedings of HCI. Sunderland, U.K.: Springer –Verlag, 2000.
[13] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy und N. Memon. Authentication using graphical passwords: Basic results. Human-Computer Interaction International (HCII 2005),2005.
[14] L. Sobrado and J.-C.Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002
[15] S. Chiasson, R. Biddle, and P. van Oorschot, “A second look at the usabilty of click-based graphical passwords,” in ACM Symposium on Usable Privacy and Security (SOUPS), July2007.