International Journal of Electrical Electronics & Computer Science Engineering
Volume 4, Issue 3 (June, 2017) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

An Amelioration Approach of Image Based Password Authentication

Praveshika Tiwari
Research Scholar, R.D Engineering College Duhai, Ghaziabad, India
tiwaripraveshika@gmail.com

Abstract: ***Current technology is more than capable of offering a secure authentication process, but users are confined in their ability to remember difficult words and form judicial decisions about security. In this thesis, both of these problems were addressed in the maturation of a new video-password scheme. Subject areas in computer security, password usability, and cognitive psychology were referenced throughout the plan procedure. Four new images based, password authentication systems are proposed here. The user survey for third and fourth schemes of password authentication based on images is presented in this dissertation. The fourth strategy was tested against character passwords of equal complexity and recall was measured over a seven-day period. The outcomes of the study indicate that a picture password system which accepts input without respect to society can be both safe and memorable. Both quality and picture passwords were randomly assigned from a password space of almost 29 billion possible passwords.***

Keywords: Authentication, Image based Password, Alphanumeric password Authentication, Security, Recognition, recall based technique.

I. INTRODUCTION

Information processing system security depends largely on passwords to authenticate the human users from attackers. The most common computer authentication method is to use alphanumerical usernames and passwords. Nevertheless, on that point are important drawbacks to this method. For example, Passwords selected by users are easy Guessed by the assailant. On the other hand , passwords which are difficult to guess are difficult to recall. To overpower this problem of low security, Authentication methods are broken by researchers that use images as password. In this research paper, we conduct a comprehensive survey of the existing graphical password techniques and provide a possible theory of our own.

Nevertheless, where text passwords involve alphanumeric and/or special keyboard characters, the idea behind graphical passwords is to leverage human memory for visual information, with the shared secret being related to or composed of images, parts of images, or cartoons. Despite the great bit of choices for authentication, text, passwords remain the most usual option for several reasons.

For instance, they are soft and cheap to implement; are familiar to essentially all users; allow users to authenticate themselves while avoiding privacy issues that have been raised about biometrics; and experience the advantage of portability without, for instance, having to carry physical tokens . However, text, passwords also suffer from both security and usability disadvantages - for instance, passwords are typically difficult to remember, and are predictable if user choice is allowed . In general, graphical passwords techniques are separated into two primary categories: recognition-based and recall based graphical techniques. In recognition based, a user is acquainted with a set of pictures and the user runs the authentication by making out and placing the images he chose during the enrollment phase. To recall based graphical password, a user is taken to regurgitate something that he made or picked out earlier during the enrollment phase. This task is based on recall based Technique.

II. AUTHENTICATION BACKGROUND

Password are the factual methodology for authenticating users for several decades, and have proven to be resilient to alter Authentication could be a method of determinative whether or not a specific individual or a creature ought to be allowed to access a system or associate application or simply associate object running during a device. Passwords square measure classified as shown in Fig.1.

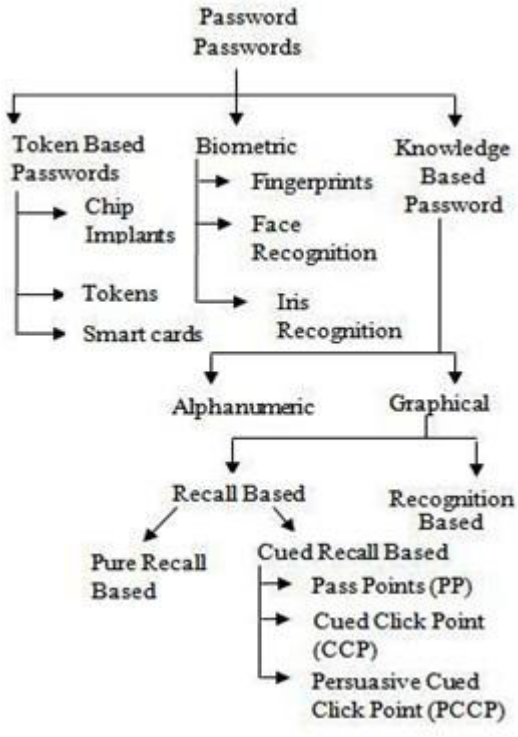


Fig. 1. Classification of Passwords

a. Token Based Password:

International Journal of Electrical Electronics & Computer Science Engineering
Volume 4, Issue 3 (June, 2017) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

Token based password, such as key cards , bank cards and fresh cards are widely practiced. Many token-based authentication systems also apply knowledge based techniques to heighten protection. For instance, ATM cards are generally used in concert with a PIN number.

b. Biometric Based Authentication:

Biometric Authentication is verification of user's identity by way of physical trait or behavioral features. It is founded on- Something You Are. It uses physiological or behavioral characteristics like a fingerprint or facial scans and iris or voice identification to identify users.

c. Knowledge based authentication:

Knowledge based techniques are the most widely used authentication techniques and include both text-based and image-based words. The image-based techniques can be further split into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is acquainted with a set of pictures and the user runs the authentication by making out and placing the images he or she selected during the enrollment phase.

Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

III. EXISTING SYSTEM

Graphical password first found in 1995 by Greg Blonder [1]. Graphical password has three types there are as follows:

1. Recognition Base Technique
2. Recall Base Technique

1. Recognition Base Technique:

Recognition base technique contain groups of pictures. User can take icons from that group for a password. Image 1 shows the recognition base technique. Using recognition base technique user set our password at the time of registration and selects same images at the time of authentication.

2. Recall Based Graphical Technique:

2.1 Pure Recall Based Technique:

This concept commencing of user producing of passwords without the system being providing of hints to produce passwords, the cases of pure recall technique are Draw-A-Secret technique, Grid selection, and Passdoodl. The coordinates of the grids occupied by the image are stored in the lodge of the draft. During authentication, the user is requested to re-delineate the picture.

If the drawing matches the same grids in the same sequence, then the user is authenticated. In this type of system the brute force attack is possible and the impact of password length and shot-count as a complexity property of the DAS system. Callback-based

graphical password schemes are on occasion named to as draw metric systems because users recall and reproduce a secret drawing.

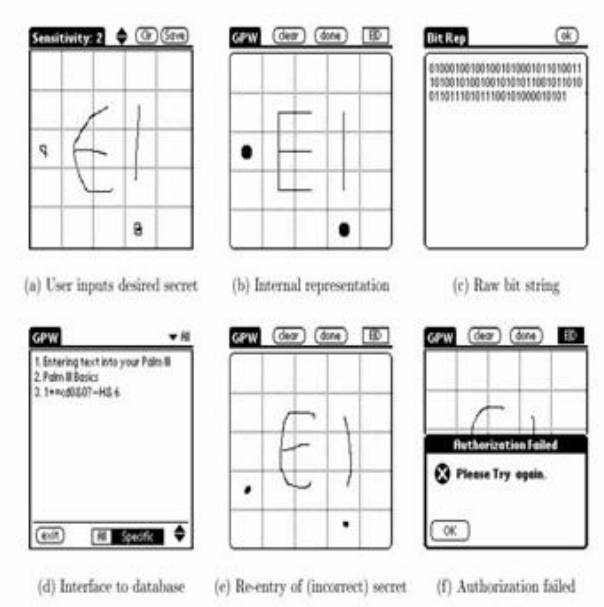


Fig.2 Draw-a-Secret (DAS) technique proposed by Jermyn

The process starts with drawing of objects or text that consist of pen strokes which is then differentiated with continuous pen stroke or several strokes that are broken up by pen ups. And so at the time of log in these sequences of coordinates of the grid cells yields an encoded DAS password.

2.2 Cued Recall-based Technique:

This technique has two implementations, PassPoints and CCP, but they result with pattern attacks and hotspots PassPoints Based on Blonder's original idea, Pass Points (PP) are a click-based graphical password scheme where a password consists of an ordered sequence of five clicks-points on a pixel-based picture. To log in, a user must click inside some system-defined tolerance region for each click-stop. The picture moves as a clue to help users remember their password click-stops. In this technique Brute force attack, hotspot attack and shape-based approaches are possible.

This technique initiates the system to provide a clue to the user that produces passwords, the system generates active areas where the user selects pixel points to choose the same region on the image following the same sequence to login into the system.

IV. PROPOSED SYSTEM DESIGN

Patrick, et al. Demonstrated that there are three central fields where human-computer relations are important:

International Journal of Electrical Electronics & Computer Science Engineering
Volume 4, Issue 3 (June, 2017) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
Available Online at www.ijeecse.com

authentication, security operations, and developing good systems. For authentication purposes, in various environments, we mostly utilize a text (alphanumeric) based password authentication mechanism.

Existing Graphical Password Schemes with their Shortcomings:

The number of Graphical password schemes is available to show their relative assessment and accountability over text based (alphanumeric) authentication. Current research and user study have shown that text-based pass-words are weighed down on the basis of memorability, usability and security problems that make them less trusted for authentication purposes. Though the text based authentication take less time for the process and occupy usually less space in memory. Dictionary attack, Brute Force Search, Guess, Spyware, Shoulder Surfing etc. are some possible password hacking mechanism may be used to crack the security based on text based authentication**.**

Click to Zoom-Inside Authentication:

The Click to Zoom-inside (CTZi) authentication is a proposed alternative to Pass Points and Cued Click Points schemes. It is a parallel research to Cued Click Point. It is a parallel research, I mean by it that we have borrowed some features from clued click point scheme and proposed a very new and high secure authentication mechanism.

WIW Scheme:

WIW Scheme The theme idea of the WIW scheme is borrowed from a well known puzzle game Where Is Waldo. In the scheme a user chooses an alphabet for his parole. At each time of login system randomly spells a string from the alphabet. A technological challenge is that it should be comfortable for the user to distinguish each of those strings and in the meantime; it is much difficult for an attacker to know any of those strings.. They are recognizable only to the user. A combination of appearances and locations of those pass-regions spells a letter. From login to login, in each theme image the locations of the pass-regions are randomly changed and their appearances are perturbed such that the letter spelled varies randomly. In this way designed scheme become secure from an attacker hardly know those letters and may film the user's login process.

Implementation of Click to Zoom-Inside (CTZi) Scheme With User Study:

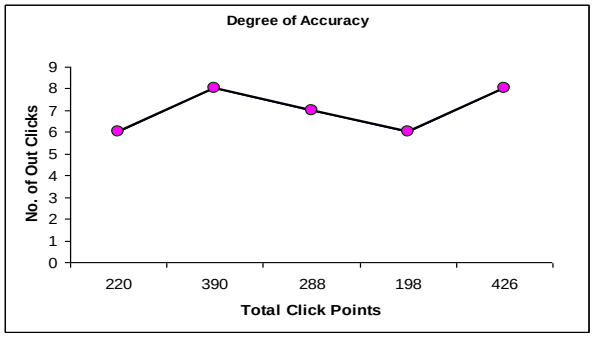
We have developed our scheme preliminarily in Computer Science Lab for Engineering Graduates of our Institute. We call this lab Network Security Lab. We have also conducted in-lab trial of our proposed scheme with 20 Computer Science Graduate students and 10 from diverse fields (but they all were regular web user); 10 of them were females and 20 males. The trial consists of one-hour session for an individual in our lab. First they all signed the consent form for the trial. They were also given printed instructions booklet for operating the system during the session. This introductory booklet included showing them an example theme image consists of several regions and how they create next image by clicking any one region on 37 the image. We also explained that the next zoom image in the sequence depended on where they clicked on the current displayed image.

V. DEGREE OF ACCURACY

The degree of accuracy can be finding by determining the maxima of the variation between the x and y coordinates of click point at the time of registration and click point at the time of login or how many click points at the time of login are out of the object region. All the click points were considered even those were unsuccessful. Analysis graph & Table 5.1 shows that there were only 12% clicks out of object region at the time of login.

Table 5.1. With Graph Showing Degree of Accuracy While Re-entering the Passwords

Login Attempts	Total Click Points	No. of Out Clicks	% of out clicks
68	220	6	2.727272727
22	390		2.051282051
80	288	7	2.430555556
41	198	6	3.03030303
41	426	8	1.877934272
Total %			**12.11734764**



VI. CONCLUSION

User authentication is a central factor in most computer security settings. In our paper, we suggested a simple graphical password authentication scheme which provides the more secure authentication than the text password scheme. We reported the system operation with the implementation of PCCP and trying to implement SHA Algorithm for folder security. PCCP tool such as PCCP's viewport (used during password creation) cannot be exploited during an approach.

VII. REFERENCES

[1] A. S. Patrick, A. C. Long, and S. Flinn, "HCI and Security Systems," presented at CHI, Extended

Abstracts (Workshops). Ft. Lauderdale, Florida, USA., 2003.

[2] A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.

[3]. A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): Springer-Verlag Lecture Notes in Computer Science (1438), 1998.

[4]. 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.

[5]. D. Davis, F. Monrose, and M.K. Reiter, "User Choice in Graphical Password Schemes", 13th USENIX Security Symposium, 2004.

[6]. G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.

[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]. J. Thorpe and P. C. v. Oorschot, "Graphical Dictionaries and the Memorable Space of Graphical Passwords," in Proceedings of the 13th USENIX Security Symposium. San Deigo, USA: USENIX, 2004.

[9]. J. Thorpe and P. C. v. Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords," in Proceedings of the 20th Annual Computer Security Applications Conference. Tucson, Arizona, 2004.

[10]. J. Goldberg, J. Hagman, and V. Sazawal, "Doodling Our Way to Better Authentication," presented at Proceedings of Human Factors in Computing Systems (CHI), Minneapolis, Minnesota, USA., 2002.

[11]. J. Thorpe, and P.C. van Oorschot, "Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords", USENIX Security Symposium, 2007 (to appear). Preliminary version available as Technical Report, TR-07-05. School of Computer Science, Carleton University, Feb. 2007.

[12]. L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[13]. L. D. Paulson, "Taking a Graphical Approach to the Password," Computer, vol. 35, 2002.

[14]. M. Kotadia, "Microsoft: Write down your passwords," in ZDNet Australia, May 23, 2005.

[15]. Passlogix, "www.passlogix.com," last accessed in June 2005.

[16]. Passfaces. http://www.realuser.com Last accessed: December 1, 2006.

[17]. R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.

[18]. RealUser, "www.realuser.com," last accessed in June 2005.

[19]. 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

[20]. Sfr, "www.viskey.com/tech.html," last accessed in June 2005.

[21]. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in Human-Computer Interaction International (HCII 2005). Las Vegas, NV, 2005.

[22]. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in Symposium on Usable Privacy and Security (SOUPS). Carnegie-Mellon University, Pittsburgh, 2005.

[23]. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human Computer Studies, to appear.

[24]. Sonia Chiason, P. C. van Oorschot and Robert Biddle, "Graphical assword Authentication using Cued Click Points", 2007. Computer Security – ESORICS 2007, vol. 4734/2007.

[25]. S. Man, D. Hong, and M. Matthews, "A Shoulder-Surfing Resistant scheme-WIW".Security and Management 2003.

[26]. T. Takada and H. Koike, "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images," in Human-Computer Interaction with Mobile Devices and Services, vol. 2795 / 2003: Springer-Verlag GmbH, 2003.

[27]. W. Jansen, "Authenticating Mobile Device Users Through Image Selection," in Data Security, 2004.

[28]. W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices," National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.

[29]. W. A. Jansen, "Authenticating Users on Handheld Devices," in Proceedings of Canadian Information Technology Security Symposium, 2003.