Survey on Various Techniques of User Authentication and Graphical Password

Miss. Saraswati B. Sahu[#1], Associate Prof. Angad Singh[*2]

1(M. Tech Scholar, Dept. of Information Technology, NIIST, Bhopal, India)
2(Associate Prof. Dept. of Information Technology, NIIST, Bhopal, India)

***Abstract*:** The process of identifying an individual usually based on a username and password. Passwords are the best commonly used method for identifying users in computer and communication systems. Usually, passwords are strings of letters and digits, i.e., they are alpha-numeric. Graphical passwords, which contain of some actions that the user accomplishes on an image.In this paper we make a survey of the basic authentication and its techniques. Survey of various techniques for authentication and password Security in a Video CAPTCHA, Persuasive Cued Click-Points Knowledge-Based Authentication Mechanism

Keywords: *Graphical password Authentication, Knowledge-Based Authentication Security, CAPTCHA, Persuasive Cued Click-Points*

1. INTRODUCTION

A password authentication system should encourage strong and less predictable passwords while maintaining memorability and security. This password authentication system allows user choice while influencing users towards stronger passwords. Social factors are often considered the weakest link in a computer security system [1]. There are three major areas where human-computer interaction is important: authentication, security operations, and developing secure systems [2]. Authentication is any protocol or process that permits one entity to establish the identity of another entity [3]. Humans have used three methods for authentication [3].
These methods are:

- Something you know (the password)
- Something you have (credit card, university ID card)
- Something you are (face, voice, signature, fingerprints, DNA, iris)

Certain disadvantages of regular password appear like stolen the password, forgetting the password, and weak password. Therefore, a large requirement to have a strong authentication method is needed to secure all our applications as possible. Conservatively, straight passwords have been used for authentication but they are known to have security and usability problems. Nowadays, other method such as graphical authentication is one of the possible substitute solutions.
Graphical password have been proposed as a possible alternative to text-based, motivated particularly by the fact that humans can remember pictures better than texts. Psychological studies have shown that people can remember pictures better than text. Pictures are generally easier to be remembered or recognized than text, especially photos, which are even easier to be remembered than random pictures [4].In graphical password, the problem arises because passwords are expected to have two fundamentals requirements, namely
a) Password should be easy to remember.
b) Password should be secured.
Graphical passwords were originally described by Blonder [7].

TAXONOMY OF AUTHENTICATION METHODS

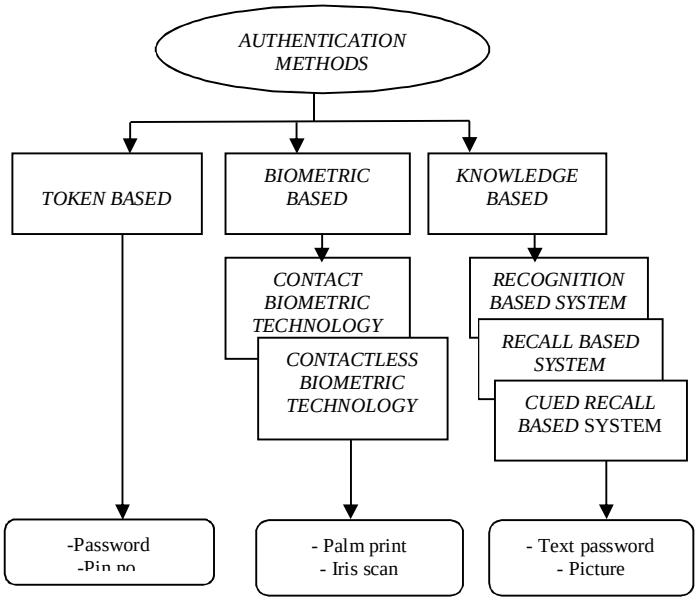

Fig 1. Taxonomy of different authentication methods

A password authentication system should encourage strong passwords while maintaining memorability. We applied this approach to create the first persuasive click-based graphical password system, Persuasive Cued Click-Points (PCCP) [5], [6]Our results show that our Persuasive Cued Click Points scheme is effective at reducing the number of hotspots (areas of the image where users are more likely to select click points) while still maintaining usability. In this paper also analyze the efficiency of tolerance value and security rate.

The remainder of this paper is structured as follows. We first discuss background literature on usable security, graphical Passwords, and persuasive technology. Next we describe our Persuasive Cued Click-Points system and methodology for the usability study. Finally we provide analysis and discussion of the results.

2. BACKGROUND

Graphical password schemes can be grouped into three general categories basedon the type of cognitive activity required to remember the password: recognition, recall, and cued recall [8].Passwords are the most prevalent user authentication method, but have security and usability problems. Replacements such as biometric systems and tokens have their own drawbacks [9], [10],[11].

2.1 Why Graphical Passwords?

Access to computer systems is most often based on the use of alphanumeric passwords. Though, users have difficulty remembering a password that is long and random-appearing. Instead, they create short, simple, and insecure passwords. Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and, therefore, more secure. Using a graphical password, users click on images rather than type alphanumeric characters.

2.2 Click-Based Graphical Passwords

Graphical password systems are a type of knowledge-based authentication that attempts to leverage the human memory for visual information. A complete review of graphical passwords is available elsewhere. Of interest here in are cued-recall click-based graphical passwords (also known as locimetric[12]). In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues[13] to aid recall. Example systems include PassPoints[14] and Cued Click-Points (CCP)[15].

In PassPoints, a password consists of a sequence of five click-points on a given image (see Figure 1). Users may select any pixels in the image as click-points for their password. To log in, they repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points. The usability and security of this scheme was evaluated by the original authors [18,19] and subsequently by others [16,17,18]. It was found that although relatively usable, security concerns remain. The primary security problem is hotspots: different users tend to select similar click-points as part of their passwords. Attackers who gain knowledge of these hotspots through harvesting sample passwords or through automated image processing techniques can build attack dictionaries and more successfully guess PassPoints passwords [17]. A dictionary attack consists of using a list of potential passwords(ideally in decreasing order of likelihood) and trying each on the system in turn to see if it leads to a correct login for a given account. Attacks can target a single account, or can try guessing passwords on a large number of accounts in hopes of breaking into any of them.

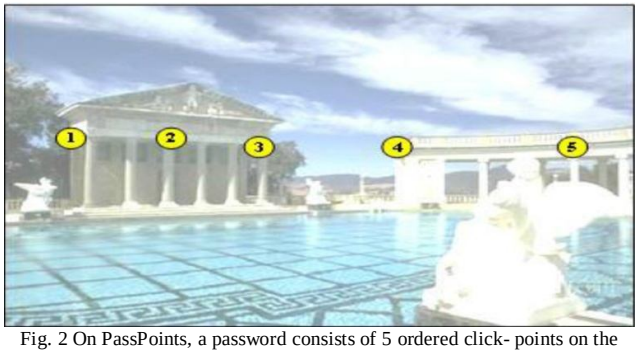

Fig. 2 On PassPoints, a password consists of 5 ordered click- points on the image Conclusions

A precursor to PCCP, Cued Click Points [18] 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 (see Figure 2), 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

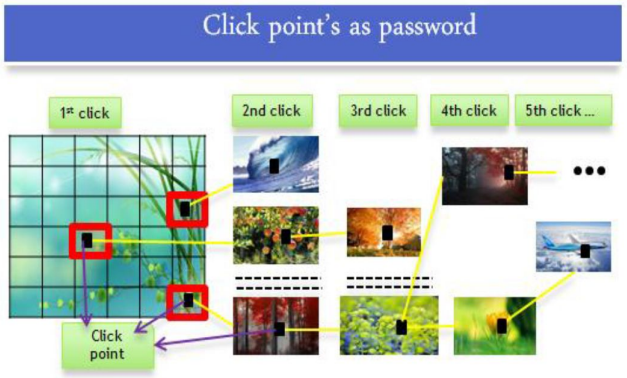

Fig. 3 with CCP, users select one click-point per image. The next image displayed is determined by the current click point.

2.3*Persuasive Technology*

Persuasive Technology was first articulated by Fogg [21] as using technology to motivate and influence people to behave in a desired manner. An authentication system which applies Persuasive Technology should guide and encourage users to select stronger passwords, but not impose system-generated passwords. To be effective, the users must not ignore the persuasive elements and the resulting passwords must be memorable. As detailed below, PCCP accomplishes this by making the task of selecting a weak password more tedious and time consuming. The path of least resistance for users is to select a stronger password (not comprised entirely of known hotspots or following a predictable pattern). The formation of hotspots across users is minimized since click-points are more randomly distributed. PCCP's design follows Fogg's Principle of Reduction by making the desired task of choosing a strong password easiest and the Principle of Suggestion by embedding suggestions for a strong password directly within the process of choosing a password.

2.4 *CAPTCHA*

A Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) is a variation of the Turing test[24], in which an online challenge is used to distinguish humans from computers. They are commonly used to prevent the abuse of online services, such as a program creating thousands of free email accounts and then using them to send SPAM. A number of hard artificial intelligence problems including natural language processing[23],character recognition [24,25],speech recognition [26] The following four desirable properties for CAPTCHAs:

1. Automated: Challenges should be easy to automatically generate and grade by a computer.
2. Open: The underlying database(s) and algorithm(s) used to generate and grade the challenges should be public. This property is in accordance with Kerckhoffs' Principle, which states that a system should remain secure even if everything about the system is public knowledge [27].
3. Usable: Challenges should be easily solved in a reasonable amount of time by humans. Furthermore, challenges should strive to minimize the effect of a user's language, physical location, education, and/or perceptual abilities.
4. Secure: Challenges should be difficult for machines to solve algorithmically.

Fig. 4Different types of CAPTCHA creator

3. PERSUASIVE CUED CLICK POINTS

Prior models have shown that hotspots are a problem in click-based graphical passwords, leading to a reduced effective password space that facilitates more successful dictionary attacks. We investigated whether password choice could be influenced by persuading users to select more random click-points while still maintaining usability.

Visual attention research [22] shows that different people are involved to the same expectable areas on an image. This suggests that if users select their own click-based graphical passwords without guidance, hotspots will remain an issue.

Davis et al. [23] suggest that user choice in all types of graphical passwords is inadvisable due to predictability.

Our goal was to encourage compliance by making the less secure task (i.e., choosing poor or weak passwords) more time-consuming and awkward. In effect, behaving securely became the path-of-least-resistance. Using CCP as a base system, we added a persuasive feature to encourage users to select more secure passwords, and to make it more difficult to select passwords where all five click-points are hotspots. Specifically, when users created a password, the images were slightly shaded except for a randomly positioned viewport (see Figure 4).The viewport is positioned randomly rather than specifically to avoid known hotspots, since such information could be used by attackers to improve guesses and could also lead to the formation of new hotspots. The viewport's size was intended to offer a variety of distinct points but still cover only an acceptably small fraction of all possible points. Users were required to select a click-point within this highlighted viewport and could not click outside of this viewport. If they were unwilling or unable to select a click-point in this region, they could press the "shuffle" button to randomly reposition the viewport. While users were allowed to shuffle as often as they wanted, this significantly slowed the password creation process. The viewport and shuffle buttons only appeared during password creation. During password confirmation and login, the images were displayed normally, without shading or the viewport and users were allowed to click anywhere.

1. Users will be less likely to select click-points that fall into known hotspots.
2. The click-point distribution across users will be more randomly dispersed and will not form new hotspots.
3. The login security success rates will be higher than to those of the original CCP system.
4. The login security success rates will increase, when tolerance value is lower value.
5. Participants will feel that their passwords are more secure with PCCP than participants of the original CCP system.

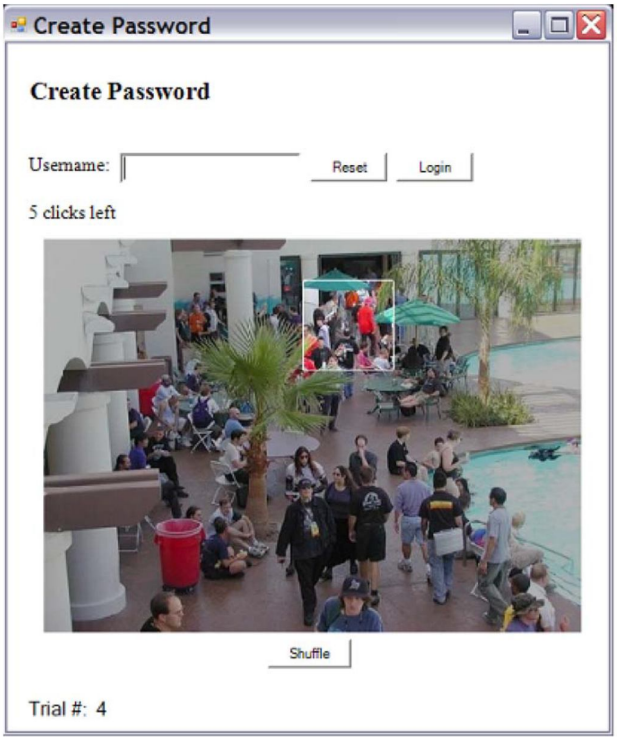

Fig. 5 PCCP Create Password interface. The viewport highlights part of the image

The theoretical password space for a password system is the total number of unique passwords that could be generated according to the system specifications. Ideally, a larger theoretical password space lowers the likelihood that any particular guess is correct for a given password. For PCCP, the theoretical password space is $((w \times h)/t2)c$ where the size of the image in pixels (w * h) is divided by the size of a tolerance square (t2), to get the total number of tolerance squares per image, raised to the power of the number of click-points in a password (c, usually set to 5 in our experiments).

In user registration module user enter the user name in user name field and also suitable tolerance value (tolerance value is use to compare registration profile vector with login profile vector). When user entered the all user details in registration phase, these user registration data stored in data base and used during login phase for verification. In picture selection phase there are two ways for selecting picture password authentication.

1. User defines pictures: Pictures are selected by the user from the hard disk or any other image supported devices.
2. System defines pictures: pictures are selected by the user from the database of the password system.

4. KNOWLEDGE BASED AUTHENTICATION

Knowledge based authentication system is an authentication system which requires the user to know something for getting the access into the system [28].

4.1 Recognition based system

Dhamija and Perrig [29] proposed a graphical authentication scheme based on the Hash Visualization technique [30]. In their system, the user is asked to select a certain number of images from a set of random pictures generated by a program. Later, the user will be required to identify the preselected images in order to be authenticated. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Weinshall and Kirkpatrick [31] sketched several authentication schemes, such as picture recognition, object recognition, and pseudo word recognition, and conducted a number of user studies. In the picture recognition study, a user is trained to recognize a large set of images (100 – 200 images) selected from a database of 20,000 images. This study showed that pictures are the most effective among the three schemes tested.

4.2 Recall Based Techniques

In this section we discuss two types of recall based techniques: reproducing a drawing and repeating a selection.

4.2.1 Reproduce a Drawing

Jermyn, et al. [32] proposed a technique, called "Draw- a -secret (DAS)", which allows the user to draw their unique password. A user is asked to draw a simple picture on a 2D grid. 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 drawing touches the same grids in the same sequence, then the user is authenticated.

4.2.2 Repeat a sequence of actions:-

Blonder [33] designed a graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas of those locations. The image can assist users to recall their passwords and therefore this method is considered more convenient than unassisted recall (as with a text-based password).

5.CONCLUSION

In this paper Authentication methods and techniques are currently available in sufficiently but each has its own profits and loss. A different authentication method is presented above. Though the main discussion for graphical based passwords is that people are better at remembering picture passwords than text based passwords, our initial analysis proposes that it is very complicated to break graphical passwords using various methods. Many researches on graphical password techniques have to be done to reach higher levels of usefulness. To conclude, we need our authentication systems to be more reliable, robust and secure as there is always a place for improvement.

REFERENCES

[1] Suo, Xiaoyuan, "A Design and Analysis of Graphical ZPassword" (2006). Computer Science Theses. Paper 27. A. C. L. Andrew S. Patrick, Scott Flinn.

[2] "HCI and Security Systems," in CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA., 2003.

[3] "Authentication Methods and Techniques", Christopher Mallow.

[4] ISO-InternationalOrganization for standardization, http://www.iso.org/iso/catalogue_detail.htm?csnumber=1688,Accessed on July 2009.

[5] S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot, "Influencing Users towards Better Passwords: Persuasive Cued Click-Points," Proc. British HCI Group Ann. Conf. People and Computers:Culture, Creativity, Interaction, Sept. 2008.

[6] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle, "Multiple Password Interference in Text and Click-Based Graphical Passwords," Proc. ACM Conf. Computer and Comm. Security(CCS), Nov. 2009.
XiaoyuanSuo, Ying Zhu and G. Scott. Owen. "Graphical passwords: a survey," Proceedings of the 21st Annual Computer Security Applications. 2005, 463-472.

[7] L. Jones, A. Anton, and J. Earp, "Towards Understanding User Perceptions of Authentication Technologies," Proc. ACM Workshop Privacy in ElectronicSoc., 2007.

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

[9] 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.

[10] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a Picture Really Worth a Thousand Words? Exploring the Feasibility of GraphicalAuthentication Systems," Int"l J. Human-Computer Studies, vol. 63, nos. 1/2, pp. 128-152, 2005.

[11] E. Tulving and Z. Pearlstone, "Availability versus Accessibility of Information in Memory for Words," J. Verbal Learning and Verbal Behavior, vol. 5, pp.381-391, 1966.

[12] S. Wiedenbeck, J. Waters, J. Birget, A. 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.

[13] 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.

[14] S. Chiasson, R. Biddle, and P. van Oorschot, "A Second Look at the Usability of Click-Based Graphical Passwords," Proc. ACM Symp. Usable Privacyand Security (SOUPS), July 2007.

[15] Golofit, K. Click Passwords Under Investigation. ESORICS 2007. LNCS 4734, 343-358, 2007.

[16] Thorpe, J. and van Oorschot, P.C. Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords. USENIX Security Symp. 2007.

[17] Wiedenbeck, S., Birget, J.C., Brodskiy, A., and Memon, N. Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. Symp. OnUsable Privacy and Security (SOUPS) 2005.

[18] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in ComputerSecurity (ESORICS), pp. 359-374, Sept. 2007.

[19] P. Dunphy, J. Nicholson, and P. Olivier, "Securing Passfaces for Description," Proc. Fourth ACM Symp. Usable Privacy and Security (SOUPS), July
2008.

[20] J. Wolf, "Visual Attention," Seeing, K. De Valois, ed., pp. 335-386, Academic Press, 2000.

[21] D. Davis, F. Monrose, and M. Reiter, "On User Choice inGraphical Password Schemes," Proc. 13th USENIX Security Symp,
2004.

[22] M. Cha, H. Kwak, P. Rodriguez, Y.-Y. Ahn, and S. Moon. ITube, You Tube, Everybody Tubes: Analyzing the World'sLargest User Generated Content Video System. In Proc. IMC2007, ACM Press (2007), 1–14.

[23] A. Rusu. Exploiting the Gap in Human and Machine Abilitiesin Handwriting Recognition for Web Security Applications.PhD thesis, University of New York at Buffalo, 2007.

[24] L. von Ahn, M. Blum, and J. Langford. Telling Humans and Computers Apart Automatically. Communications of the ACM 47, 2 (2004), 56–60.

[25] G. Kochanski, D. P. Lopresti and C. Shih. Using a Text-to-Speech Synthesizer to Generate a Reverse Turing Test. In Proc. ICTAI 2003, IEEE Press (2003), 226-232.

[26] A. Kerckhoffs. La CryptographieMilitaire. Journal des Sciences Militaires 9, (1883), 161–191.

[27] "Enhanced Knowledge Based Authentication Using Iterative Session Parameters", Ali Alkhalifah, Geoff D.Skinner, World Academy of Science, Engineering and Technology 47 2010

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

[29] 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

[30] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.

[31] 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, 2012

[32] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 2009