Available online at www.ijiere.com
International Journal of Innovative and Emerging Research in Engineering
e-ISSN: 2394 – 3343 p-ISSN: 2394 – 5494

Three Level Security Using Cued Click Points in Image Based Authentication

Ankit Aggarwal, Darshil Doshi, Vijay Gore and Jignesh Sisodia
Information Technology Dept., Sardar Patel Institute of Technology, Andheri (W), Mumbai, India

ABSTRACT:
Providing a security to the information system is the necessity of today's networking age. A graphical based authentication mechanism had provided a strong alternative for knowledge based, biometric and token based authentication mechanism. In this project we have developed unique user- friendly System named as 3 Level Security that can be employed in any organization for ensuring its security through its three levels– which are Text based password, image based password and One Time Automated Password which presents unique and an esoteric study of using images as password and implementation of an extremely secured system, utilizing 3 levels of security.

Keywords: Graphical password, OTP, Cued points, authentication.

I. INTRODUCTION

As the internet becomes more prominent, need for passwords increases, the question arises as to whether the current text based password is a competent and safe solution to security system in the future [2]. Moreover, even away from internet, due to increased intrusions into computer system, the password is an area of predominant authentication on the internet. With the conventional content based way to passwords, the exchange off in the middle of convenience and security has not so far been valuable to clients. As Bill Gates said at a security gathering

"There is no doubt that over time people are going to rely less and less on passwords. People use the same password on different systems, they write them down and try just don't meet the challenge for anything you really want to secure" (Fraser 2006)

The requirement for more secure passwords that are non- word reference, non-individual and solid alphanumeric has implied that the customary password has their own decision is liable to start passwords that are considered frail by today's standard and leave their security open to attack by intruders. Graphical passwords can be classified into three types: Draw-based type, choice based type, click-based type. In draw-based type, users have to draw some secrete. In Choice-based type, users have flexibility to select sequence of images to set the password. In the case of click-based method, a user has to select click points on the image [5].

Psychology studies have uncovered that human brain is better at perceiving and reviewing pictures than content. Graphical passwords were proposed to profit by this human trademark with the expectation that by decreasing the memory trouble on clients, coupled by bigger gull password space offered by pictures, more secure passwords can be created. Moreover picture based password System is extremely financially savvy as the primary structure of the framework is not bargained. The venture includes execution of three level validation utilizing content based, picture based and OTP interfaces to assess their adequacy into this present reality circumstances

II. AIM AND OBJECTIVE

Authentication is a procedure of figuring out if a specific individual or a gadget ought to be permitted to get to a framework or an application or only an item running in a gadget. This is a critical methodology which guarantees the essential security goals[6]. On the web, pernicious clients or projects may endeavor to acquire touchy data disturb administrations or produce information by mimicking substantial elements is the part of validation and is key to system security[16].Validation includes affirming the character of a man or programming project, following the cause of a relic, or guaranteeing that an item is what is bundling and naming cases to be. It is performed by evaluation of credentials supplied by user [2]. In this framework we coordinates the security procedures of content based password , Image based password authentication and one time secret key .The point of the venture is to propose a basic yet secure and easy to understand verification strategy consequently lessening the powerlessness of the programmer sniffing system activity and impeding shoulder and brute force attack on the client side.

III.LITERATURE SURVEY

Dhamija and Perrig[9] proposed a graphical authentication plan in light of the Hash Visualization technique[10]. In this system, the client is solicited to choose a specific number from pictures from an arrangement of arbitrary pictures produced

by a project. At that point the client will be verified by method for recognizing the preselected pictures. This strategy neglects to inspire in light of the fact that the server needs to store the seeds of the portfolio pictures of every client in plain content. Akula and Devisetty's[9] calculation is like the procedure proposed by Dhamija and Perrig[14]. The distinction is that by utilizing hash calculation SHA-1, which creates a 20 byte yield, the confirmation is more secure and requires less memory. The creators proposed a conceivable future change by giving diligent stockpiling and this could be conveyed on the Internet, mobile phones and PDAs. Weinshall and Kirkpatrick [12] outlined a few confirmation plans, for example, picture recognition, object recognition, and pseudo word recognition, and led various client studies. In the photo recognition mull over, a user is prepared to perceive a substantial arrangement of pictures, chosen from a database of 20,000 pictures. This study uncovered that photos are the best among the three plans examined. Jansen et al[11] proposed a graphical password mechanism for mobile devices. During the enrolment stage, a user selects a theme (e.g. sea, cat, etc.) which consists of thumbnail photos and then registers a sequence of images as a password. Amid the confirmation, the client must enter the enlisted pictures in the right arrangement. One disadvantage of this procedure is that since the quantity of thumbnail pictures is restricted to 30, the password space is less. Every thumbnail picture is doled out a numerical worth, and the succession of choice will produce a numerical secret key. The outcome delineated that the picture succession length is for the most part shorter than the printed secret key length. To address this problem, two pictures can be combined to compose a new alphabet element, thus expanding the image alphabet size [13]. Takada and Koike talked about a comparable graphical secret word method for cell phones. This system permits clients to utilize their most loved picture for validation [14].The customers first enroll their most cherished pictures (pass-pictures) with the server. In the midst of acceptance, a customer needs to experience a couple of rounds of check. At each round, the customer either picks a pass-picture among a couple of diversion pictures or picks nothing if no pass-picture is accessible. The framework sanctions a customer just if all affirmations are compelling. Permitting clients to enlist their own particular pictures makes it less demanding for client to recollect their password pictures. This system is a protected verification technique in examination with content based passwords. much all the more Allowing clients to utilize their own particular pictures would make the secret key unsurprising, particularly if the aggressor is acquainted with the client.

IV. PROPOSED SYSTEM

Now-a-days, all business, government associations and academic associations are contributing a great deal of time, money and PC memory for the security of data. Information security is basic for most organizations and even home PC clients. Client information, portion information, individual archives, money related equalization unpretentious components - most of this information can be hard to supplant and possibly dangerous in case it falls into the wrong hands.Data misfortune because of debacles, for example, a surge or flame is squashing, yet losing it to programmers or a malware disease can have much more prominent outcomes [7]. This proposed system also gives insurance against key logger as computer mouse is issued instead of the console to enter our graphical password; this shields the password from key loggers.

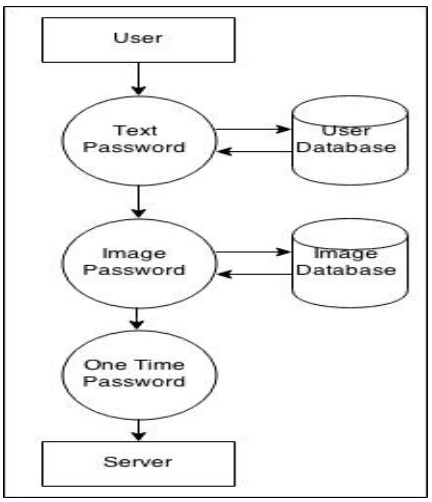

Figure 1: Architecture Diagram

V. PROPOSED SYSTEM

Now In this section we discuss three types of security password techniques:

A. Text Based Authentication (Level 1):

This level deals with the normal text based password creation i.e. the client side is ensured by the use of text password, and that text password has to be entered by ensuring employment of special characters[3]. This is the normal text-based user login which the users are familiar with. During authentication, the user again enters this password to gain access to the second level.

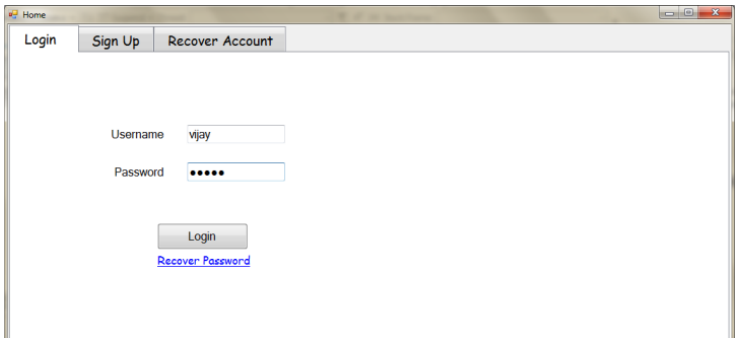

Figure 2: Text Based Authentication

B. Graphical Password (Level 2)

Graphical passwords were first described by Blonder. His concept is mainly based on click points on predefined areas of image. And as this scheme forces user to click on predefined areas this scheme is vulnerable to predictive attacks. Later Wiedenbeck et al. proposed PassPoints. Passpoints consists of passwords that could be composed of several points anywhere on an image [15]. Most graphical password systems are based on either recognition or cued recall [4]. In recognition-based systems the user must recognize previously chosen images from a larger group of distracter images. The decision is binary: either the image is known (recognized) or not known. In cued recall password systems users must click on several previously chosen areas in an image, cued by viewing the image. Both types of systems may have memory advantages over alphanumeric passwords [8]. Here the user is presented with three images. The user is asked to select one point per image during registration which will be used during authentication Then during authentication, when the user encounters the same image which he/she had seen during registration, it triggers the memory of which point the user clicked. The system provides a degree of tolerance, i.e., the user is allowed to click around 9-10 pixels around the point on which the user clicked during registration. The accuracy findings for click points provide further evidence that tolerance squares as small as of 9x9 pixels may be acceptable terms of usability [1]. If the user click is within the level of tolerance, the user is presented with the next proper image, otherwise the user is shown a random image, which an authentic user will immediately come to know about. Here, the hacker won't get a clue about a correct or an incorrect image, whereas an authentic user will know about it and he/she can restart the authentication process.

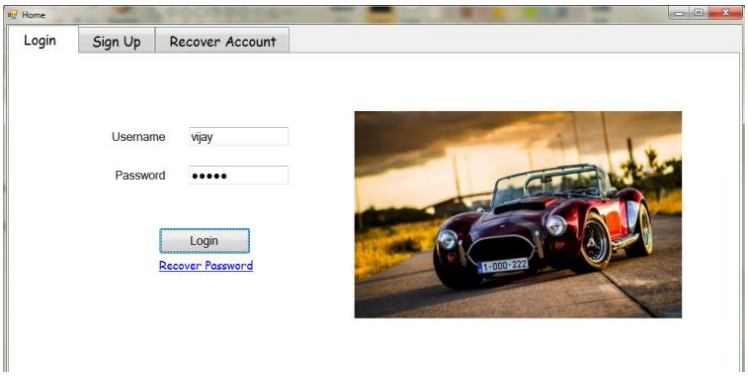

Figure 3: Image Based Authentication

C. OTP Based Authentication (Level 3)

Here the user will be sent a randomly generated one time password via email or SMS. This will have to be entered by the user to gain access to the system. One-time password schemes are relevant primarily for network settings, to defend against the threat of a network eavesdropper capturing password information in transit between the user and a secure authentication server. To render such eavesdropping harmless, a one-time password scheme varies the user's password from each login to the next in a way that only the user and the server can predict [4].

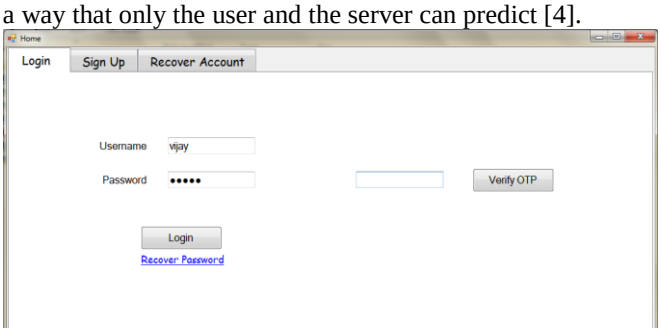

Figure 4: OTP Based Authentication

VI. CONCLUSION

A typical security objective in password based authentication frameworks is to boost the compelling secret word space. The three level security methodology connected on the above framework, makes it profoundly secure alongside being more client friendly.3-Level Security framework is certainly a period expending methodology, as the client needs to cross through the three levels of security, and will need to allude to his email-id for the one-time computerized created secret word. Hence, this framework can't be a suitable answer for general security purposes, where time unpredictability will be an issue. But will most likely be an aid in regions where high security is the fundamental issue, and time multifaceted nature is optional, as an illustration we can take the instance of a firm where this framework will be available just to some higher assignment holding individuals, who need to store and keep up their critical and private information secure.

REFERENCES

[1] Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. ACM Computing Surveys (CSUR), 44(4), 19.

[2] Chiasson, S., Forget, A., Biddle, R., & van Oorschot, P. C. (2008). Influencing users towards better passwords: Persuasive cued click- points. Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction-Volume 1, 121-130.

[3] De Angeli, A., Coventry, L., Johnson, G., & Renaud, K. (2005). Is a picture really worth a thousand words exploring the feasibility of graphical authentication systems. *International Journal of Human- Computer Studies, 63*(1), 128-152.

[4] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin, The Design And Analysis Of Graphical Passwords,Proceedings of the 8th USENIX Security Symposium

[5] Washington, D.C., USA, August 23–26, 1999. S. Chiasson, R. Biddle, and P. van Oorschot. A second look at the usability of click-based graphical passwords. In the proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS), July 2007.

[6] van Oorschot, P. C., & Thorpe, J. (2011). Exploiting predictability in click-based graphical passwords. *Journal of Computer Security, 19*(4), 669-702.

[7] Security Implementation of 3-Level Security System Using Image Based Authentication M.Manjunath, Mr. K. Ishthaq Ahamed and Ms. Suchithra.International journal of engineering trends and technology in computer science (IJETTCS) Volume 2, Issue 2, March – April 2013.

[8] An Image Based Approach For Authentication Using Multi-Level Security System Kiran, . Purushotham, Dilli Kumar. International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106 Volume- 1, Issue-7, Sept-2013

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

[10] 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.

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

[12] 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.

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

[14] 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, pp. pp. 347 - 351.

[15] Active Image Authentication System (AIAS): Design, Implementation and Analysis .S.B.Nikam, P.A.Jadhav and A.D.Kadam. International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 2, Issue 11, November 2013 ISSN 2319 – 4847 Volume 2

[16] Security Analysis & It's Implementations Using Image Based Authentication for 3-Level Security.System .Rahul S. Mate, Pramod P. Gadekar, Suhas B. Sathe, Prof. Mangesh K. Manke