ISSN:2320-0790

An International Journal of Advanced Computer Technology

Graphical Password Authentication Scheme Using Cloud

Vijayshri Vaidya

Abstract: Graphical password is one of the alternative solutions to alphanumeric password as it is very tedious process to remember alphanumeric password. When any application is provided with user friendly authentication it becomes easy to access and use that application. One of the major reasons behind this method is according to psychological studies human mind can easily remember images than alphabets or digits. In this paper we are representing the authentication given to cloud by using graphical password. We have proposed cloud with graphical security by means of image password. We are providing one of the algorithms which are based on selection of username and images as a password. By this paper we are trying to give set of images on the basis of alphabet series position of characters in username. Finally cloud is provided with this graphical password authentication.

Keywords: Graphical passwords, PCCP, Cloud, authentication, Security

I. INTRODUCTION

Today computer has become a integral part of our day today life. The computer applications from all sorts of areas from business to banking and many more. The applications hold data and details of all the transaction a organization does. So to protect the applications authentication techniques like textual passwords with various strengths are used which help to protect a application.The vulnerabilities of textual password to method like eves dropping, dictionary attack, social engineering and shoulder surfing are well known. Random and lengthy passwords can make the system secure. But the main problem is the difficulty of remembering those passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can be easily guessed or cracked. Biometric based authentication and

Knowledge based authentication. Most of the web application provides knowledge based authentication which include alphanumeric password as well as graphical password. In today's changing world when we are having number of networks and personal account some sort of easy authentication schema need to be provided. This paper is based on securing cloud by using graphical password. Cloud security can also be givenby alphanumeric password but thing matter is that use of alphanumeric is not that much of secure.

II. LITERATURE SURVEY:

Graphical password is an alternative solution to secure system rather than text based password. Reason behind is graphical pictures are more easily recalled than text. Graphical password schemes can be grouped into three general categories: recognition based, pure recall based, and cued recall based techniques.

Click-based graphical passwords:

Graphical password systems are a type of knowledge-based authentication that attempt to leverage the human memory for visual information. A comprehensive review of graphical passwords is available elsewhere. Of interest herein are cued-recall click-based graphical passwords (also known as loci metric). In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues to aid recall. Example systems include PassPoints and Cued Click Points . In PassPoints, passwords consist of a sequence of five click-points on a given image. Users may select any pixels in the image as click-points for their password. To log in, they repeat the sequence of cicks in the correct order, within a system-defined tolerance square of the original click-points. Although PassPoints is relatively usable security weaknesses make passwords easier for attackers to predict. Hotspots are areas of the image that have higher likelihood of being selected by users as password click-points. Attackers who gain knowledge of these hotspots through harvesting sample passwords can build attack dictionaries and more successfully guess PassPoints passwords Users also tend to select their click-points in predictable patterns (e.g., straight lines), which can also be exploited by attackers even without knowledge of the background image; indeed, purely automated attacks against PassPoints based on image processing techniques and spatial patterns are a threat . A precursor to PCCP, Cued Click-Points (CCP) 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 (Figure 1), 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. The claimed advantages are that password entry becomes a true cued-recall scenario, wherein each image triggers the memory of a corresponding clickpoint. Remembering the order of the click-points is no longer a requirement on users, as the system presents the images one at a time. CCP also provides implicit feedback claimed to be useful only to legitimate users. When logging on, seeing an image they do not recognise alerts users that their previous click-point was incorrect and users may restart password entry. Explicit indication of authentication failure is only provided after the final click-point, to protect against incremental guessing attacks. User testing and analysis showed no evidence of patterns in CCP , so pattern-based attacks seem ineffective. Although attackers must perform proportionally more work to exploit hotspots, results showed that hotspots remained a problem.

Persuasive Technology:

Persuasive Technology was first articulated by Fogg [22] 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 timeconsuming. 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.

III. PROPOSED SYSTEM

Persuasive Cued Click-Points (PCCP) [1][8] is a variation of CCP designed to persuade users to select more random passwords. It functions like CCP, but during password creation the image is blurred except for a small square viewport area randomly positioned on the image. Users select a click-point from within this viewport (see fig 4), or may press a \shuffle" button to randomly reposition the viewport until a suitable location is found. On subsequent logins, images are displayed in their normal format with no blur or viewport. Common perception that users choose the path-of-least-resistance here means selecting a click-point within the first or first few viewports. The design intent of the viewport is to pattern the distribution of click-points across multiple users, reducing hotspots and pattern formation.

PCCP:

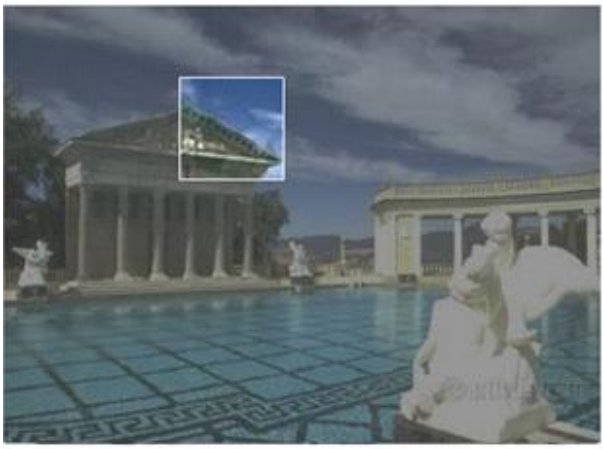

Fig 4: PCCP

Different users might be select same images. Same images could be reused by two different users, highest probability of collision may be occurs. With the help of inclusion-exclusion principle will be minimized. PCCP reportedly removes major concerns related to common patterns and hotspots. PCCP use a grid-based discreatization algorithm to find out whether login click-points are within that tolerance area. In system-side storage for verification, these passwords can be hashed; additional information such as a grid identifier (for each click-point), however, is stored in a manner accessible to the system, to allow the system to use the appropriate grid to verify login attempts. It is unclear if attackers gaining access to the server-side storage can use these grid identifiers to their advantage.

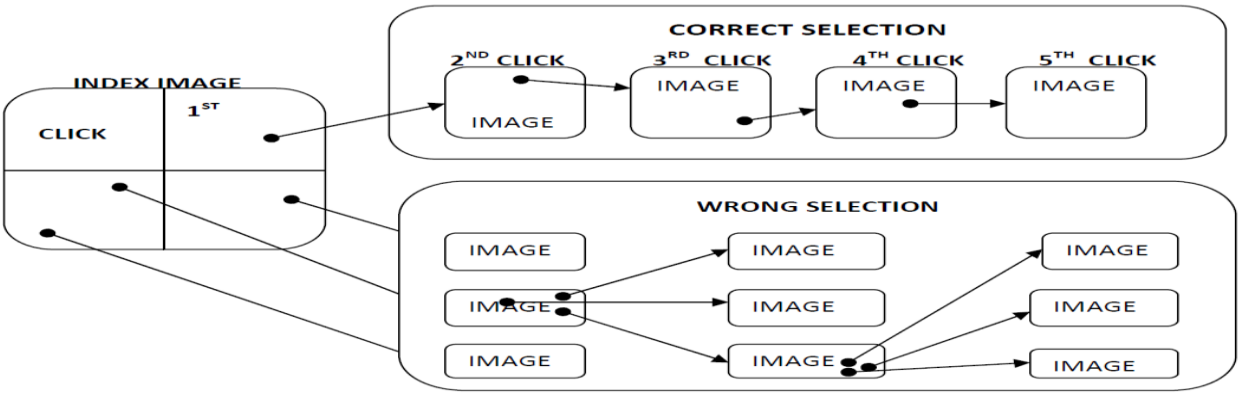

Fig. 7. PCCP selection technique

IV. ADVANTAGES

Graphical password provides more security than alphanumeric password. Most of the alphanumeric authentication choose a plain text or easy password to avoiding the confusion. whenever we confirm the alphanumeric password there is some hint option provided, using this hackers can easily gain entry to the system in less time. Most of the system provides image related password i.e. Graphical password. In this method selectable images are used , user can have more number of images on each page and among all of this password is selected. Images are different for each case, so if hackers try to match the each combination to find the correct password it will take millions of year. In alphanumeric password eight characters password is needed to gain entry of particular system, but in graphical password user have to select the images that in front of him/her and confirm the password. Whenever user pass through the authentication process it is easy to remember images whatever they have chosen previously. Graphical password is providing more memorable password than alphanumeric password which can reduce theburden on brain of user.

V. REFERENCES

[1] A Survey on Recognition-Based Graphical User Authentication Algorithms FarnazTowhidi Centre for Advanced Software Engineering, University Technology Malaysia Kuala Lumpur, Malaysia.

[2] Authentication Using Graphical Passwords: Basic Results Susan Wiedenbeck Jim Waters ,College of IST Drexel University Philadelphia, PA, 19104 USA.

[3] Security Analysis of Graphical Passwords over the Alphanumeric Passwords by G. Agarwal ,1Deptt.of Computer Science, IIET, Bareilly, India 2,3 Deptt. of Information Technology, IIET, Bareilly, India 27-11-2010.

[4] Graphical Passwords,FABIAN MONROSE AND MICHAEL K. REITER,August 5, 2005 Networks J., vol. 4, no. 5, pp. 567-585, Sept. 2006.

[5] A Survey on Recognition-Based Graphical User Authentication Algorithms Network Protocols and Algorithms, vol 3, no. 4, pp. 122-140, 2011.

[6] Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice Susan Wiedenbeck Jim Waters College of IST Drexel University Philadelphia.

[7] Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme Susan Wiedenbeck and Jim Waters College of IST Drexel University Philadelphia, PA 19104 USA.

[8] Graphical Passwords as Browser Extension: Implementation and Usability Study1,Kemal Bicakci1, Mustafa Yuceel1, Burak Erdeniz2, Hakan Gurbaslar2, NartBedin Atalay3.

[9] Pass-Go, a New Graphical Password Scheme,HAITAOThesis submitted to the Faculty of Graduate and Postdoctoral Studies Electrical and Computer Engineering University of Ottawac Hai Tao, Ottawa,Canada, June, 2006.

[10] Graphical Password Authentication system in an implicit manner,SUCHITA SAWLA*, ASHVINI FULKAR, ZUBIN KHAN Department of Computer Science, Jawaharlal Darda Institute of Engineering Technology, Yavatmal, MS, India. March 15, 2012.

[11] Authentication for Session Password Using Colour and Images by jai patel,SNJB's COE Computer Engineering Department, University Of Pune. Ganeshkhind,Pune.