Implementation Of Knowledge Based Authentication System Using Persuasive Cued Click Point

Mrs.M.L.Prasanthi, Devi Srinivas
Associate Professor Computer Science and Engineering Vardhaman College of Engineering Hyderabad
Computer Science and Engineering Vardhaman College of Engineering Hyderabad

Abstract-Now-a-days, as information systems are open to the Internet, the importance of security for Networks are tremendously increased. Usable security has unique usability challenges because the need for security often means that standard human computer interaction approaches cannot be directly applied. An important usability goal for a authentication systems is to support users in selecting better passwords. Users often create memorable passwords that are easy for attackers to guess but strong system assigned passwords are difficult for users to remember. So researchers of modern days have gone for alternative methods. Here a graphical password system with One Time Password (OTP) is discussed. In proposed work a click-based graphical password scheme called Persuasive Cued Click Points (PCCP) is presented. In this system a password consists of sequence of some images in which user can select one click-point per a specific region of an image. In addition user receives an OTP through Email in order to verify himself to the system. The OTP is generated using random algorithm by which it is make unique for each and every time the user requests for logins. If the user chooses the correct click a point on each region of set of images chosen and has to verify the OTP sent to him in order to access his Information. System showed very good Performance in terms of speed, accuracy, and ease of use. Users preferred PCCP to Pass Points, saying that selecting and remembering only one point per image was easier.

Keywords: Security, Graphical password, Persuasive Cued Click Points.

INTRODUCTION

It is now beyond any doubt that USER AUTHENTICATION is the most critical element in the field of Information Security. To date, Text Based Password Authentication (TBPA) has shown some difficulties that users have tended to write passwords down manually or save them on hard disc. This tendency is caused by passwords being strong and thus difficult to memorize in most cases. This has inadvertently given rise to security issues pertaining to attack. Graphical User Authentication (GUA) has two symbiotic pillars as its foundation: USABILITY &SECURITY. The macro-concept of GUA is based on the human psychological factor that is images are more readily committed to memory than would TBPA's.

Undoubtedly, there is currently the phenomenon of threats at the threshold of the internet, internal networks and secure environments. Although security researchers have made great strides in fighting these threats by protecting systems, individual users and digital assets, unfortunately the threats continue to cause problems. The principle area of attack is AUTHENTICATION, which is of course the process of determining the accessibility of a user to a particular resource or system.

Today, passive or active users are the key consideration of security mechanisms. The passive user is only interested in understanding the system. The active user, on the other hand, will consider and reflect on ease of use, efficiency, Memorability, effectiveness and satisfaction of the system. Generally, authentication methods are classified into three categories:

A). Inherit Based Authentication

The Inherent Based Authentication category which is also known as Biometric Authentication, as the name suggests, is the automated method/s of identity verification or identification based on measurable physiological or behavioral characteristics such as fingerprints, palm prints, hand geometry, face recognition, voice recognition and such other similar methods. Biometric characteristics are neither duplicable nor transferable. They are constant and immutable. Thus it is near impossible to alter such characteristics or fake them. Furthermore such characteristics cannot be transferred to other users nor be stolen as happens with tokens, keys and cards. Unlike the security of a user's password, biometric characteristics, for instance the user's fingerprint or iris pattern, are no secret. Hence there is no danger of a break in security.

B). Token Based Authentication

The Token Based Method category is again as the name suggests authentication based on a TOKEN such

as: a key, a magnetic card, a smart card, a badge and a passport. Just as when a person loses a key, he would not be able to open the lock, a user who loses his token would not be able to login, as such the token based authentication category is quite vulnerable to fraud, theft or loss of the token itself.

C). Knowledge Based Authentication

The concept of Knowledge Based Authentication is simply the use of conventional passwords, pins or images to gain access into most computer systems and networks. Textual (alphabetical) and graphical user authentications are two methods which are currently used. True textual authentication which uses a username and password has inherent weaknesses and drawbacks which will be discussed in the following section.

2. BACKGROUND

One of the major problems of the textual password is the difficulty of remembering passwords. A survey has shown that most of the users tend to select short passwords or passwords that are easy to remember which unfortunately, can be easily guessed or broken by attackers. Other users select long passwords which are difficult to commit to memory, as well as hard to guess or break. The other drawback with textual passwords is that most users cannot remember a number of passwordsfor different authentications; they tend to use the same passwords for different accounts. Survey done by Xiaoyum at 2005 has revealed that running a password cracker in a sample network uncovered about 80% of passwords in 30 seconds (Xiaoyuan et al. 2005).Psychological confirmed that, people can recognize and remember combinations of geometrical shapes, patterns, textures, and colors better than meaningless alphanumeric characters, making the graphical user authentication to be greatly desired as a possible alternative to textual passwords. This type of authentication is formed by combining images, icons or pictures.

3.3 Recall based techniques

In this section we discuss recent types of click based graphical password techniques:

1. Pass Points (PP)
2. Cued Click Points (CCP)
3. Persuasive Cued Click-Points (PCCP)

3.3.1 Pass point (PP)

3. Graphical Password Systems

Graphical passwords were first Described By Blonder.Since then, many other graphical password schemes have been proposed. Graphical password systems can be classified as either recognition-based (image based scheme, cued recall-based (image based scheme) or pure recall-based (grid based scheme).

3.1 Recognition Based Techniques

3.1.1 Dhamijaand Perrig

Dhamija and Perrig proposed a graphical authentication scheme based on the Hash Visualization technique. In their system Figure2: 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. Weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plaintext. Also the process of selecting a set of pictures Akula and Devisetty's algorithm is similar to the technique proposed by Dhamija and Perrig. The images will be converted into hashing codeusingSHA-1 techniques to give more secure and less memory. This Technique produces a 20 byte output .Both the above algorithms are prone to shoulder surfing attacks.

3.2.2 Hong'sMethods

Hong, eta Proposed another shoulder-surfing resistant algorithm. In this approach to allow the user to assign their own codes to pass object variants. Fignre3: shows the log-in screen of this graphical password scheme. However, this method still forces the user to memorize many text strings and therefore suffer from the many drawbacks of text-based passwords.

Based on Blonder's original idea, Pass Points (PP) is a click- based graphical password system where a password consists of an ordered sequence of five click-points on a pixel-based image as shown in Figure.4Tolog in; a user must click within some system-defined tolerance region for each click-point. The image acts as a cue to help users remember their password click-points.

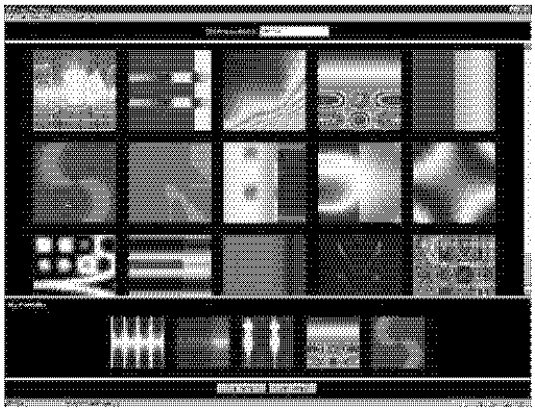

Figure3: Login Screen

3.3.2 CuedClickPoints (CCP)

CCP was developed as an alternative click based graphical password scheme where users select one point per image for five images Figure.5: The interface displays only one image at a time; the image is replaced by the next image as soon as a user selects a click point. The system determines the next image to display based on the user's click-point on the current image. The next image displayed to users is based on a deterministic function of the point which is currently selected. It now presents a one to-one cued recall scenario where each image triggers the user's memory of the one click- point on that image. Secondly, if a user enters an incorrect click-point during login, the next image displayed will also be incorrect. Legitimate users who are an unrecognized image know that they made an error with their previous click-point. Conversely, this implicit feedback is not helpful to an attacker who does not know the expected sequence of images.

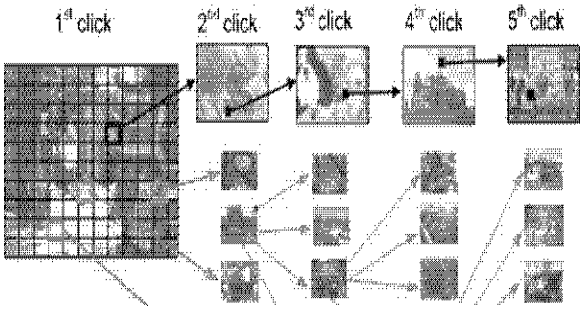

Figure 4: Cued Click Points

3.3.3 PersuasiveCuedClick Points (PCCP)

To address the issue of hot spots, PCCP was proposed as with CCP, a password consists of five click points, one on each of five images. During password creation, most of the image is dimmed except for a small view port area that is randomly positioned on the image as shown inFigure.5.Usersmustselecta click-point within the view port. If they are unable or unwilling to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots. A user who is determined to reach a certain click-point may still shuffle until the view port moves to the specific location, but this 1s a time consuming and more tedious process.

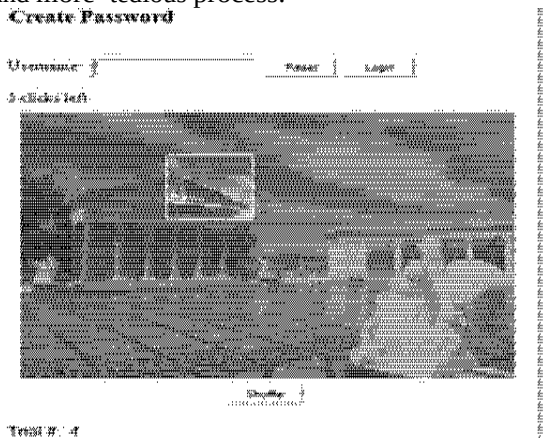

Figure6: the PCCP password

4. PROPOSED SYSTEM

Now-a-days, all business, government, and academic organizations are investing a lot of money, time and computer memory for the security of information. Online password guessing attacks have been known since the early days of the Internet, there is little academic literature on prevention techniques. This project deals with guessing attacks like brute force attacks and dictionary attacks.

This project proposes a click-based graphical password system. During password creation, there is a small view port area that is randomly positioned on the image. Users must select a click-point within the viewport. If they are unable to run willing to select

appoint in the current viewport, they may press the Shuffle button to randomly reposition the viewport. The viewport guides users to select more random passwords that are less likely to include hotspots. Therefore this works encouraging users to select more random, and difficult passwords to guess. Brute force and dictionary attacks on password-only remote login services are now wide spread and ever increasing. Enabling convenient login for legitimate users while preventing such attacks is a difficult problem Automated Turing Tests (ATTs) continues to be an effective, easy-to-deploy approach to identify automated malicious login attempts with reasonable cost of inconvenience to users. This project proposes a new Password guessing Resistant Mechanism prior proposals designed to restrict such attacks. While PGRP limits the total number of login attempts from unknown remote hosts, legitimate users in most cases (e.g., when attempts are made from known, frequently-used machines) can make several failed login attempts before being challenged with an ATT. This proposed system also provides protection against key logger spy ware. Since, computer mouse issued rather than the keyboard to enter our graphical password; this protects the password from key loggers.

5. CONCLUSION & FUTURE WORK

Common security goals in password-based authentication systems are to maximize the effective password space. This impacts usability when user choice is involved. We have shown that it is possible to allow user choice while still increasing the effective password space. Furthermore, tools such as PCCP's viewport (used during password creation) cannot be exploited during an attack. Users could be further deterred (at some cost in usability) from selecting obvious click-points by limiting the number of shuffles allowed during password creation or by progressively slowing system response in repositioning the viewport with every shuffle past a certain threshold. The approaches discussed in this paper present a middle ground between insecure but memorable user-chosen passwords and secure system generated random passwords that are difficult to remember. Providing instructions on creating secure passwords, using password managers, or providing tools such as strength meters for passwords have had only limited success. The problem with such tools is that they require additional effort on the part of users creating passwords and often provide little useful feedback to guide users' actions. InPCCP, creating a less guessable password (by selecting a click-point within the first few system-suggested viewport positions) is the easiest course of action. Users still make a choice but are constrained in their selection. Another often cited goal of usable security is helping users from accurate mental models of security. Through our

Guiding users in making more secure choices, such as using the viewport during password creation, can help foster more accurate mental models of security rather than vague instructions such as "pick a password that is hard for others to guess." This persuasive strategy has also been used with some success to increase the randomness of text passwords. Better user interface design can influence users to select stronger passwords. A key feature in PCCP 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 patterns, thus increasing the effective password space.

6. ACKNOWLEDGMENT

I would like to express my sincere thanks to my guide and my authors for their consistence support and valuable suggestions.

7. REFERENCES

[1]Sonia Chiasson, P.C.van Oorschot, and Robert Biddle,"Graphical Password Authentication Using Cued Click Points" ESORICS, LNCS4734,pp.359-374, Springer Verlag Berlin Heidelberg 2007.

[2]Manu Kumar,Tal Garfinkel, Dan Bonehand Terry Wino grad, "Reducing Shoulder-surfing by Using Gaze based Password Entry", Symposium on Usable Privacy and Security (SOUPS), July 18-20, 2007, Pittsburgh, PA, USA.

[3]ZhiLi, QibinSun, Yong Lian, and D.D. Giusto, 'An association-based graphical password desigu resistant to shoulder surfing attack', International Conference on Multimedia and Expo (ICME), IEEE.2005

[4]R.Dhamija and A.Perrig, "Deja Vu:A User Study Using Images for Authentication", in *Proceedingsoj9thUSENIX* Security Symposium, 2000.

[5]S.Akula and V.Devisetty, "Image Based Registration and Authentication System", in *Proceedings ojlv1idwes Instruction and Computing Symposium* 2004.

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

[7]Sonia Chiasson, Alain Forget, Robert Biddle,P.C. van Oorschot,"User interface desigu affects security: patterns
in click-based graphical passwords", Springer Verlag
2009.

[8]I.Jermyn,A.Mayer,F.Monrose,M.K.Reiter and D.Rubin, "The Desigu and Analysis of Graphical Passwords,"in *Proceedings of the 8thUSENIX Security Symposium*,1999.

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

[10]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.

[11]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.

[12]E. Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords," Proc. Ann. Computer Security Applications Conf. (ACSAC), 2010.

[13]S.Chiasson, A.Forget,R.Biddle, and P.C. van Oorschot,"User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords," Int'l J. Information Security, vol. 8, no. 6, pp. 387-398, 2009.