Implementation Of Multi Level Security System Using Click Based Authentication.

Mr. K. Ishthaq Ahamed, M. Manjunath,

Associate professor Dept of Computer Science and Engineering, G.Pulla Reddy Engineering College (Autonomous), Kurnool, Andhra Pradesh, India.

M .Tech (C.S.E) G.Pulla Reddy Engineering College (Autonomous), Kurnool, Andhra Pradesh, India.

Abstract

*Now a days, as information systems are more open to the Internet, the importance of security for networks is 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 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 Onetime 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 a 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 us*e. *Users preferred PCCP to Pass Points, saying that selecting and remembering only one point per image was easier.*

1. 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 passwords for 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. 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:

3.1.1Dhamija and Perrig

Dhamija and Perrig [4] proposed a graphical authentication scheme based on the Hash Visualization technique. In their system Figure 2: 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 pre-selected 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. Also, the process of selecting a set of pictures Akula and Devisetty's algorithm [5] is similar to the technique proposed by Dhamija and Perrig. The images will be converted into hashing code using SHA-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's Methods

Hong, et a!. [7] Proposed another shoulder-surfing resistant algorithm. In this approach to allow the user to assign their own codes to pass-object variants. Figure 3: 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.

3.3 Recall based techniques:

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

1.Text Authentication (LEVEL-1)

2. Image Authentication (LEVEL-2)

3. OTP Authentication (LEVEL-3)

3.3.1 Text Authentication (LEVEL-1)

Passwords have been used with computers since the earliest days of computing. MIT's CTSS, one of the first time sharing systems, was introduced in 1961. It had a LOGIN command that requested a user password. "After typing PASSWORD, the system turns off the printing mechanism, if possible, so that the user may type in his password with privacy. To log in, at 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. Therefore, security at LEVEL1 is ensured by use of text password which is a usual approach with normal login scheme.

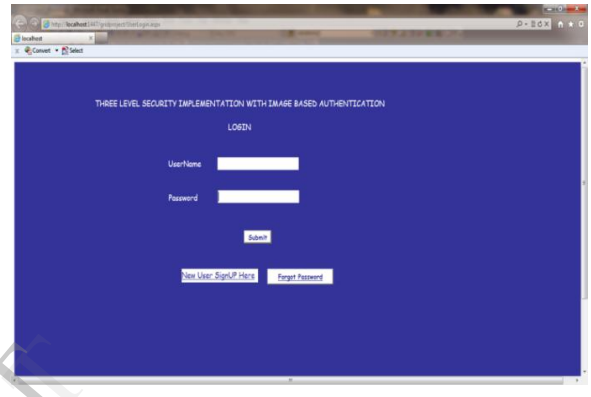
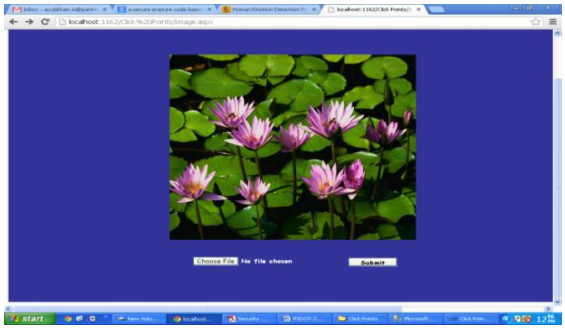


Figure 1: Login Screen

3.3.2 Image Authentication (LEVEL-2)

Image based authentication was developed as an alternative click based graphical password scheme where users select three click points on image for one image Figure.4: The interface displays only one image at a time; the image is uploaded as soon as a user selects a click point and pixel points are saved for next login authentication. The system determines the next pixel point based on the user's click-point on the current image and deterministic function of the point which is currently selected. **It** now presents a one-to-many cued recall scenario where 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 click point displayed will not be considered. Conversely, this implicit feedback is not helpful to an attacker who does not know the expected click points on image.



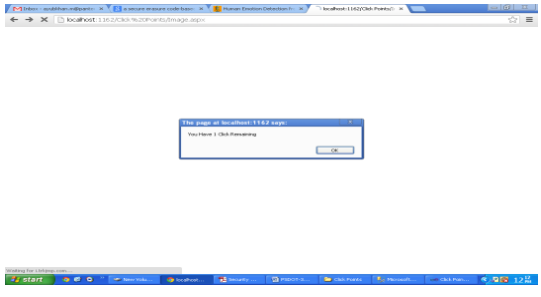
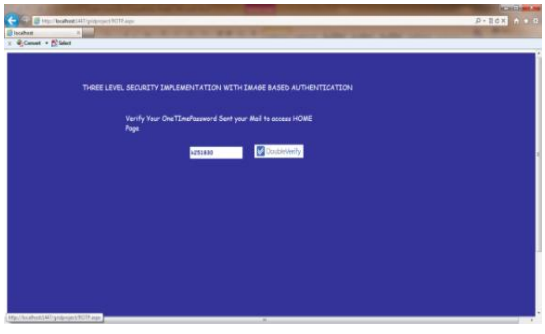


Figure 2: Click Points



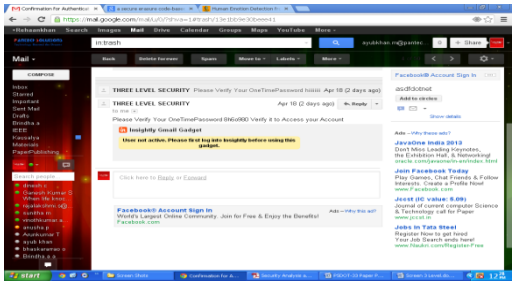


Figure 3: OTP Password

3.3.3 OTP Authentication (LEVEL-3)

3rd LEVEL security has been imposed by generating a onetime random code. This random code or can say the password will be generated each time during the specific login session, for the user to login to his account after the successful completion of two authentication processes (security level1- Text password and security level2-Image based authentication). This unique code will be updated in the database on the server. And the user will be informed of this one-time password through an automated email. This will definitely help in thwarting Brute force attack (can be attempted upon the previous two security levels), as this unique one-time password will be send on user's email-id saved in the database. And the user will be granted access to that one-time password, only upon having access to that email-id. Therefore, the hacker if successful(although difficult) to cross through the above two mentioned security levels, will definitely not be able to cross the third security level, unless he has access to the original user's email-id.

4. Proposed System

Now-a-days, all business, government organizations 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 3 levels of security. During password creation, there is an image user will select three click points or pixel positions within that image. After considering the pixel positions user must relogin and authenticate for the next level of login process i.e., OTP generation sent to the E-mail ID. Therefore this works encouraging users to select Image and difficult Click points to guess.

Brute force and dictionary attacks on password-only remote login services are now widespread and ever increasing. Enabling convenient login for legitimate

users while preventing such attacks is a difficult problem. Automated Turing Tests (ATTs) continue 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

A common security goal in password-based authentication systems is 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, OTP Generation done by random number generator algorithm (used during password creation) cannot be exploited during an attack. 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. In Image Based authentication, creating a less guessable password (by selecting a click-point within that image) 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.

The three level security approach applied on the above system, makes it highly secure along with being more user-friendly.3-Level Security system is definitely a time consuming approach, as the user has to traverse through the three levels of security, and will need to refer to his email-id for the one-time automated generated password. Therefore, this system cannot be a suitable solution for general security purposes, where time complexity will be an issue. But will definitely be a boon in areas where high security is the main issue, and time complexity is secondary, as an example we can take the case of a firm where this system will be accessible only to some higher designation holding people, who need to store and maintain their crucial and confidential data secure.

Acknowledgement

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

References

[1] Sonia Chiasson, P.C. van Oorschot, and Robert Biddle, "Graphical Password Authentication Using Cued Click Points" ESORICS, LNCS 4734, pp.359-374, Springer Verlag Berlin Heidelberg 2007.

[2] Manu Kumar, Tal Garfinkel, Dan Boneh and Terry Winograd, "Reducing Shoulder-surfing by Using Gazebased Password Entry", Symposium On Usable Privacy and Security (SOUPS) , July 18-20, 2007, Pittsburgh,PA, USA.

[3] Zhi Li, Qibin Sun, 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 *Proceedings oj9th USENIX 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, A l a i n Forget, Robert Biddle, P. C. van Oorschot, "User interface design affects security: patterns in click-based graphical passwords", Springer-Verlag 2009.

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

[9] S. Chiasson, R. Biddle, and P. van Oorschot, "A Second Look at the 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.