International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 4, April - 2013

Graphical Based Password Authentication

Alankrita Ladage
Student

Swapnil Gaikwad
Student

Prof. A. B.Chougule
Professor

Abstract

This paper presents the implementation of pass points, cued click points and in a queue for implementation subjected to its execution of persuasive cued click-points considering security .The major goal of this work is to reduce the guessing attack by using Persuasive Technology that should guide users to select stronger passwords. Persuasive Technology influences user to select more difficult password for secure authentication.

1. Introduction

Because of increasing threats to networked computer systems, there is great need for security innovations. Authentication refers to the techniques where users have to prove the claim of their identity to the identifier. Users can be authenticated in one of the following three ways: i) what they know (e.g., password) ii) what they have (e.g., smart card) and iii) what they are (e.g., biometrics). Commonly used authentication schemes are password based schemes Passwords are text passwords or graphical passwords. But text or alphanumeric passwords are mostly easy and short but have their own problems too. Natural tendency of the users that they will always prefer to go for short passwords for ease of remembrance and also lack of awareness about how attackers tend to attacks. Unfortunately, these passwords are broken mercilessly by intruders by several simple means such as masquerading, Eaves dropping and other rude means say dictionary attacks, shoulder surfing attacks, social engineering attacks. Alternatively Graphical passwords[2] have a predetermined image that the sequence and the tap regions selected are interpreted as the graphical password Graphical passwords are uncommon and cost effective. Psychology studies have revealed that the human brain is better at recognizing and recalling images than text. Graphical passwords are sequence of pictures which are more memorable than a sequence of characters. Pictures are independent from user's language. There do not exist yet special dictionaries for a dictionary attack and it are very difficult to be constructed and automated attacks are difficult to take place.

2 Background

2.1 Problems with text passwords

Text passwords represent the authentication method that is mainly used by all users today. Nevertheless, most times users select passwords that are memorable and as a result easy to be cracked. Some of the usual problems are the following: Passwords are very short in length. Passwords are easy to remember. Passwords are writing down or share with others, in order to remember them easier. Use the same passwords for different applications. Security depends on the users' ability to maintain the password secret. Not fully reliable when used for making financial transactions remotely, such as fund transfers and bill payments through an Internet banking channel.

2.2 Need for Graphical Password

Passwords require the user to protect the user name and password from unauthorized use. If not protected, accounts and files can be compromised. Hence an improved system and method is needed to create password values that are both exceedingly difficult for an intruder to compromise, while simultaneously easy for a user to apply and maintain. Most graphical

password systems[4] are based on either recognition or cued recall. 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

3.Graphical Password Techniques

In general, the graphical password techniques [7] can be classified into two categories: recognition-based and recall-based graphical techniques

3.1Recognition Based System

In recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. There are many recognition based schemes. Some of them are is PassFac-es which was developed by Real User Corporation . Another recognition-based scheme is Pass-Objects which was developed by Sobrado and Birget [6]. Although a recognition-based graphical password seems to be easy to remember, which increases the usability, it is not completely secure. Also, it is obvious that recognition based systems are vulnerable to replay attack and mouse tracking because of the use of a fixed image as a password

3.2 Pure Recall-based Techniques

In this group, users need to reproduce their passwords without any help or reminder by the system. Draw-A-Secret technique [8], Grid selection [3], and Passdoodle [5] are common examples of pure recall-based techniques.

3.3 Cued Recall-based Techniques

In this technique, the system gives some hints which help users to reproduce their passwords with high accuracy. These hints will be presented as hot spots (regions) within an image. The user has to choose some of these regions to register as their pass-word and they have to choose the same region following the same order to log into the system. The user must remember the “chosen click spots” and keep them secret. There are many implementations, such as Blonder scheme and PassPoint scheme .

4. System Architecture

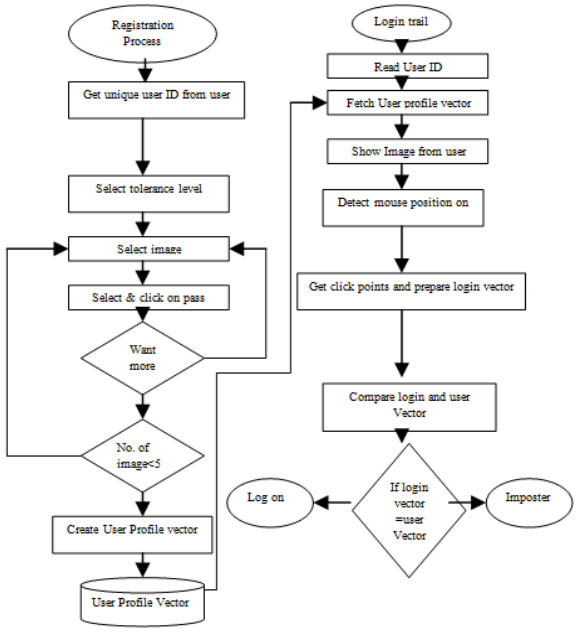

Figure 1: System Architecture

System Architecture is an conceptual model to define structure,behavior and more views of a particular system.Its vital to see that the modern system architecture did not appear out. Although it depends largely on practices and techniquies which developed over period of time in other fields.

5. Proposed Work

We are going to implement the following aspects in login process of a website or web application:

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

5.1 Pass Points (PP)

- Pass Points (PP)[1] is a click-based graphical password system where a password consists of an ordered sequence of five click-points on a pixel-based image.

- To log 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. Cue is a signal, such as a word or action used to prompt another event in a performance.

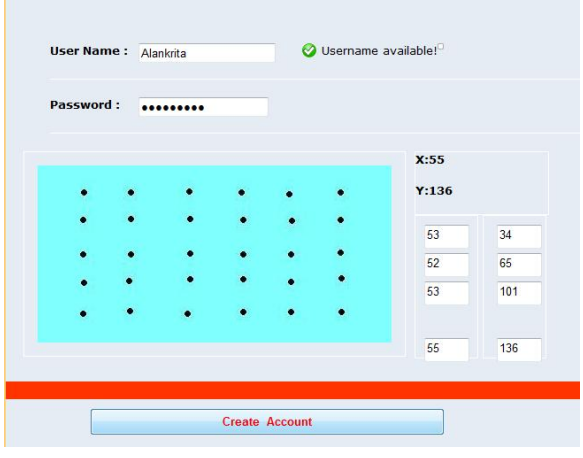

Figure 2. Login through Pass point

Figure 3. Login successful through Pass points

5.2 Cued Click Points (CCP):

- 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 see 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

In this module we implement the cued click point technique in which user navigates through number of images. The next image is displayed according to the previous images' click point.

5.3 Persuasive Cued Click-Points-(PCCP)

While implementing Pass-Points and cued click points[3] the guessing attacks, capture attack, and hotspot problems which reduces the security of graphical password schemes and to overcome this We are trying to implement persuasive cued click points in which 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.Users must select a 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 viewport moves to the specific location. Viewport is nothing but a framed area

6. Persuasive Technology

Persuasive Technology used to motivate and influence people to behave in a desired manner. Persuasive Technology was first articulated by Fogg. An authentication system which applies Persuasive Technology should insist users to select stronger passwords. PCCP's[8] 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.

7. Security

PCCP's resistance to standard security threats: guessing attacks and capture attacks.

7.1 Guessing Attacks

The most basic guessing attack against PCCP is a brute force attack and dictionary attacks. Brute Force Attack: A Brute Force attack is a type of password guessing attack and it consists of trying every possible code, combination, or password until you find the correct one. This type of attack may take long time to complete. A complex password can make the time for identifying the password by brute force long. Dictionary Attack: A dictionary attack is another type of password guessing attack which uses a dictionary of common words to identify the user's password

7.2 Capture Attacks

Password capture attacks occur when attackers directly obtain passwords by intercepting user entered data, or by tricking users into revealing their passwords. The attacker's task is more difficult for PCCP because not only is the popularity of hotspots reduced, but the sequence of images must be determined and each relevant image collected, making a customized attack per user

7.3 Hotspots

Hotspots are specific areas in the image that have a higher probability of being selected by users as part of their passwords. If attackers can accurately predict the hotspots in an image, then a dictionary of passwords containing combinations of these hotspots can be built. Hotspots are known to be problematic for PassPoints

Conclusion

User authentication is a fundamental component in most computer security contexts. In this extended abstract, we proposed a simple graphical password authentication system which provides the more secure authentication than the text password scheme. We described the system operation with implementation of pass points and cued click points and highlighted important aspects of the system. And trying to implement persuasive cued click point based scheme to minimize the security related problem arises with pass points and cued click points.

ACKNOWLEDGMENT

I would like to express my gratitude and appreciation to all those who gave me the possibility to complete this paper. A special thanks to our final year project coordinator, whose help, stimulating suggestions and encouragement, helped me to coordinate my project especially in writing this paper.

REFERENCES

[1] S.Wiedenbeck, J.Waters, J. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, 2005.

[2] K. Golofit, "Click passwords under investigation," in 12th European Symposium on Research in Computer Security (ESORICS), LNCS 4734, September 2007.

[3] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using Cued Click Points," in European Symposium on Research in Computer Security (ESORICS), LNCS4734, September 2007.

[4] R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Computing Surveys (to appear), 2012.

[5] P. C. van Oorschot and J. Thorpe, "Exploiting predictability in click-based graphical passwords," Journal of Computer Security, 2011.

[6] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on PassPoints-Style graphical passwords, "IEEE Trans. Info. Forensics and Security, vol. 5, no. 3, pp. 393–405, 201

[7] Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Exploring usability effects of increasing security in click-based graphical passwords," in Annual Computer Security Applications Conference (ACSAC), 2010.

[8] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. van Oorschot, "Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism," School of

Computer Science, Carleton University,Tech. Rep. TR-11-03, February 2011.

[9] P. C. van Oorschot and J. Thorpe, "Exploiting predictability in click-based graphical passwords," Journal of Computer Security,vol. 19, no. 4, pp. 669–702, 2011.