THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Graphical Password Authentication: Personalized Cued Click Points to overcome the limitations of Persuasive Cued Click Points

Victor Fernandes
BE Computer Engineering Department
St. Francis Institute of Technology, Mumbai, Maharashtra, India
Sweedal Lopes
BE Computer Engineering Department
St. Francis Institute of Technology, Mumbai, Maharashtra, India
Parima Gavaskar
BE Computer Engineering Department
St. Francis Institute of Technology, Mumbai, Maharashtra, India

Abstract:
With the rising amount of transactions and activities done online, almost every site requires user authentication. Along with the convenience of having everything online also comes the risk of having all your privileged and confidential data being either stolen or misused. We will be studying the various authentication schemes being used today and also their strengths and limitations. This paper focuses on using a slightly modified version of Cued Click points referred to as Personalized Cued Click points instead of Persuasive cued click points and the aim of this paper is to propose a future-proof method that would easily adapt into the existing systems available today while enhancing the security and making it easier to remember as well. Personalized cued click points also prevents hotspots and Brute-force attacks. We suggest using personalized cued click points which is capable of eliminating all of the above limitations.

Keywords*: authentication, computer security, graphical passwords, guessing attacks and centered discretization, cued click points*

1. Introduction

In recent years passwords have become the dominant means of access control to online services. Almost every site has all confidential data under a password. Most people normally do not take online security as a serious subject. For example, most users do not take the strength of the password as a serious topic while signing up for an email. One may argue what one can do by assessing my email. I do not have anything to hide there, it's just filled with spam newsletters and a few friendly messages. However one must understand that email hacks are a much bigger problem than you think.[2] So the solution to all these demands remains simple, find an authentication method that would prove to be safe and easy to remember. Human factors are often considered the weakest link in any authentication system.[4]

1.1 What are passwords?

Oxford dictionary defines passwords as "A secret word or phrase that must be used to gain admission to a place"[1]

1.2. Why Personalized Cued Click Points

We believe that a new authentication scheme must be adaptable enough to merge with any existing authentication scheme. Also we wanted the scheme to be as easy and quick as possible and also wanted it to have high security. Replacements such as biometric systems and tokens have their own drawbacks [7] [8], [9]. Personalized Cued click points proved to fit into every requirement. People sometimes confuse or mix-match freely the terms 'security' and 'privacy[6].

1.3. Is GPA as secure as the conventional Alpha Numeric Password?

Very little research has been done to study the difficulty of cracking graphical passwords. Because graphical passwords are not widely used in practice, there is no report on real cases of breaking graphical passwords. Here we briefly exam some of the possible techniques for breaking graphical passwords and try to do a comparison with text-based passwords.

- **Brute force search:** The main defense against brute force search is to have a sufficiently large password space. Text-based

Passwords have a password space of 94^N, where N is the length of the password, 94 is the number of printable characters excluding SPACE. Some graphical password techniques have been shown to provide a password space similar to or larger than

that of text-based passwords.[3] Recognition based graphical passwords tend to have smaller password spaces than the recall based methods.

1.4. Acknowledgement

We would like to express our special thanks of gratitude to our project guide Ms. Ankita R Karia (Lecturer, St Francis Institute of Technology) for her help and support while researching on the subject. We would also like to mention that this would not be possible without the unity and cooperation of the authors Victor Fernandes, Sweedal Lopes and Parima Gavaskar.

2. Literature Review

In this section we shall review the various existing password schemes and also their limitations. We will also learn about the various attacks that need to be overcome.

2.1. Classification of Authentication methods

Security being such an important aspect of any system, the authentication system had to be developed more and more over the years. The primary function of the authentication system is to successfully process information such that it can verify the true identity of a person or system. As of now there are three main types of Authentication schemes: Token based (two factor), Biometric based (three factor), and Knowledge based (single factor) authentication.

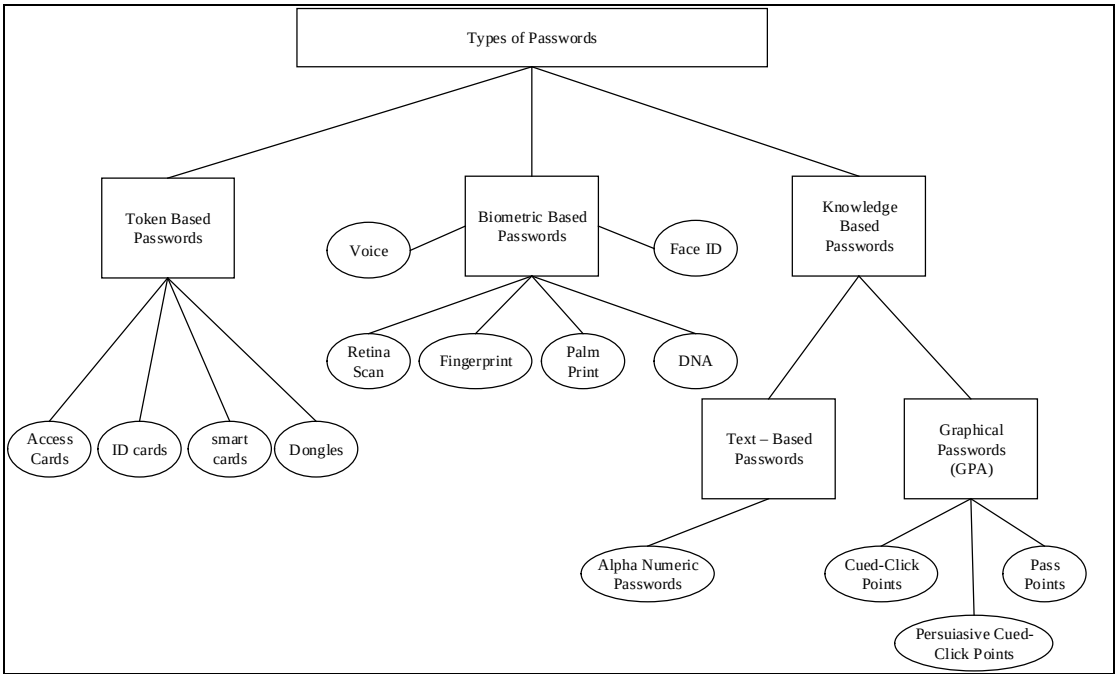

Chart 1

2.1.1. Token Based Authentication method

A token is a physical object that you can carry along with you. The simplest example of a token based password is a university identity card. A student is only required to carry it along with him/her and he is automatically allowed to enter the institute on the basis of the card possession. More examples include Smart Cards, a driver's license, and credit cards. Now consider this situation: You lost your credit card on your way to work. Someone finds it and instead of returning it to the bank he uses the card. The merchant establishments, where the card is being used do not question the card holder for further details such as the bank account number or personal details as everything is already available on the card. The person thus is successful in using your identity and authenticating as you without your presence. This is one of the major drawbacks of this system.

- **Benefits:** It increases security as compared to passwords, no need to remember anything.
- **Cons:** Can be lost/stolen, Observable and possible to replicate, Accessibility.

2.1.2. Biometric Based Authentication scheme

This authentication scheme refers to the identification of humans by their characteristics and traits. One way to look at is by asking the human what are the distinctive and measurable characteristics that can be used to label oneself. It uses characteristics like fingerprints or retina scans in order to identify the person. Biometric identification depends on computer algorithms to make a yes/no decision. The different types of biometric authentication methods are as below.

Contact metric technologies:	Contact less technologies:
Finger print	Facial recognition
Hand/Finger geometry	Voice recognition
Dynamic signature verification	Iris scan
Keystroke dynamics	Retinal scan

- **Benefits:** Highest Level of Security, Positive and accurate identification, safe and user friendly, nothing to remember or carry.
- **Cons:** Susceptible to replay-capture of data and reuse, Biometric systems are expensive, Unreliable, Perceived privacy threats.

2.1.3. Knowledge based Authentication schemes

In this scheme, the user is required to prove his identity by providing some information that is stored in the memory of the user. Basically it is something you remember that is used to authenticate you. Codes such as PIN (Personal Identification number), text based passwords and Graphical Passwords.

KBA is often used as a component in multifactor authentication (MFA) and for self-service password retrieval and offers several advantages to traditional (conventional) forms of e-authentication like passwords, PKI and biometrics (Kba 2011). It can be divided into three sub types as follows:

- Recognition based systems
- Recall based systems
- Cued recall based systems

Our main topic of interest would be the various existing Graphical Password Authentication schemes available.

- **Pass points:** In the pass point authentication scheme, the user clicks on multiple pixels on the screen to set it as his password. There is a tolerance value around each pixel calculated. In order to authenticate, the user needs to click on the appropriate pixel within the image in the correct sequence.
- **Dhamija and Perrig Scheme:** In this scheme, the user is requested to pick out of many pictures out of several choices. The user needs to identify them later during authentication.
- **Passface scheme:** In the passface scheme, the faces of people are used as a password. The user needs to identify these faces later to authenticate.
- **Sobrado and Birget Scheme:** In this scheme, the system displays a number of pass-objects which were pre-selected by the user. The user is supposed to click inside the convex hull bounded by the pass-objects.
- **Cued Click Points:** In Cued click points there are a number of images used. During the registration phase, the user clicks on a point on an image and he is taken to another image, he again repeats this step for a predetermined number of images.[5] During the authentication phase the user is required to select on the appropriate pixels and based on a suitable tolerance value. If the pixel is correct, the user is authenticated. One of the major drawback of this system is Hot Spots which is taken care of by using Personalized Cued Click Points.
- **Persuasive cued Click Points:** In Persuasive Cued Click Points, the system presents a view port to the user in addition to the process in cued click points, this fairly reduces the problem of hot spots. This however also makes the password moderately difficult to remember as the viewport is no longer visible during the authentication phase.

3. Our Proposal

As we have seen above, Persuasive Cued Click points does solve the problem of hotspots, however raises a bigger problem, i.e. remembering the point. The user may tend to find it frustrating that the password is so difficult to keep in mind. In order to overcome these limitations we recommend using Personalized Cued Click Points.

3.1. The Concept

The basic concept of using Personalized Cued Click points is that the user decides what images are displayed during the authentication phase. These images may have a particular importance or memory associated with it which is known only to the user and not an attacker. For example, the user may upload a map of his home town and the point he selects would be the place he bought his first car or the place his childhood school, etc. Other possibilities include a family function where he selects a point on his favorite dish on the table, etc. The possibilities are high and so is the security. This does solve the problem of hotspots as the user is not forced to select an image that is unknown to him. Also, using this scheme, there is no possible way an attacker can perform a brute-force attack.

4. Design and Implementation

Figure 1: Sample Screen of Personalized Cued Click Points

4.1. Registration Phase (Signup)

During the registration phase, the user first needs to set his unique user name. Once that is set, he is given an option to upload his first image. Next he selects a particular pixel on the image. This image and the pixel coordinates are encrypted and stored in the database. The user does these steps for 5 images. Once these 5 images and their coordinates are saved in the database, the registration phase is complete. It is very important for the user to remember both, the approximate pixel position and the sequence of the image

4.2. Authentication Phase (Login)

During the authentication phase, the user is requested to first enter his username. The user is then presented with the first image he used during the signup process. Then he needs to select an approximate pixel position on his screen. There is 5% tolerance accepted. This means if the user's image is 640x480 and his pixel position is (100,100), the system will accept any values between (68 to 132, 68 to 132) pixel position.

One of the most important feature of this system is that if the user inputs the wrong pixel, he does not get a direct prompt saying the point is incorrect. Instead, he gets another image next instead of the one he expects. This is to be understood as a sign that the previous point entered is wrong. Each image will have the button "Wrong Image?" which upon clicking takes the user to the previous image to re select the image. Alternatively the user can also start over from the 1st image by selecting the "Start Over" button.

If the user selects a pixel on a wrong image, i.e. the image shown after he wrongly enters the previous image's pixel, the particular username gets blocked for 2 hours and a continue link is emailed the user along with an attacker alert notification.

5. Conclusion

There is a growing demand of the use of Graphics instead of Text as passwords however there has been no method found yet to be as easy to remember as the conventional alpha-numeric text based passwords. Every authentication scheme has its own advantages and disadvantages. The main reason Graphical Passwords came into existence was since it could be easily recalled. This was the main disadvantage with Persuasive Cued Click points. We believe that Personalized Cued Click points will prove to be an easy and more secure alternative to the currently being used alpha-numeric text based passwords.

6. References

1. Definition of password in English (Oxford): http://www.oxforddictionaries.com/definition/english/password
2. E-mail Hacks - A Bigger Problem than you Think http://www.securityweek.com/e-mail-hacks-bigger-problem-you-think
3. Graphical Passwords: A Survey: Xiaoyuan Suo Ying Zhu G. Scott. Owen Department of Computer Science Georgia State University.
4. A. S. Patrick, A. C. Long, and S. Flinn, "HCI and Security Systems," presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA., 2003.
5. GRAPHICAL AUTHENTICATION USING REGION BASED GRAPHICAL PASSWORD, G. NIRANJANA & KUNAL DAWN

6. Security still not taken seriously on the Web: study http://www.itworldcanada.com/article/security-still-not-taken-seriously-on-the-web-study-2/39230
7. L. Jones, A. Anton, and J. Earp, "Towards Understanding User Perceptions of Authentication Technologies," Proc. ACM Workshop Privacy in Electronic Soc., 2007.
8. L. O"Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91, no. 12, pp. 2019-2020, Dec. 2003.
9. A. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Trans. Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125-143, June 2006