Knowledge Based Authentication Mechanism Using Persuasive Cued Click Points

Tara H R
Dept. of ISE, Sambhram Institute of Technology (VTU), Bangalore

Usha T
Dept. of ISE, Sambhram Institute of Technology (VTU), Bangalore

Ganeshayya I Shidaganti
Lecturer, Dept. of ISE, SaIT, Bangalore

Abstract

This paper presents an integrated evaluation of the Persuasive Cued Click-Points graphical password scheme including implementation considerations. An important usability goal for knowledge-based authentication systems is to support users in selecting passwords of higher security, in the sense of being from an expanded effective security space. We use persuasion to influence user choice in click-based graphical passwords, encouraging users to select more random and hence more difficult to guess, click-points. Graphical passwords essentially use images or representation of images as passwords. Human brain is good in remembering picture than textual character. There are various graphical password schemes or graphical password software in the market. However, very little research has been done to analyze graphical passwords that are still immature. Therefore, this paper work uses the persuasive cued click-points method.

1. Introduction

Persuasive Cued Click-Points scheme is effective at reducing the number of hotspots (areas of the image where users are more likely to select click points) while still maintaining usability. We find that graphical passwords offer an excellent environment for exploring strategies for helping users select better passwords since it is easy to compare user choices.

The remainder of this paper is organized as follows. We first discuss about the three different authentication methods and then about click-based graphical passwords. Finally we discuss about the persuasive technology.

Graphical passwords offer an alternative to text-based passwords that is intended to be more memorable and usable because graphical passwords rely on our ability to more accurately remember images than text.

We focus primarily on click-based graphical passwords. In *Pass Points*, 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 clicks in the correct order. Each click must be within a system-defined tolerance region of the original click-point. The usability and security of this scheme was evaluated by the original authors and subsequently by others .It was found that although relatively usable, security concerns remain. The primary security problem is hotspots: different users tend to select similar click-points as part of their passwords. Attackers who gain knowledge of these hotspots through harvesting sample passwords or through automated image processing techniques can build attack dictionaries and more successfully guess Pass Points passwords. A dictionary attack consists of using a list of potential passwords (ideally in decreasing order of likelihood) and trying each on the system in turn to see if it leads to a correct login for a given account. Attacks can target a single account, or can try guessing passwords on a large number of accounts in hopes of breaking into any of them. To reduce the security impact of hotspots and further improve usability, we proposed an alternative click-based graphical password scheme called *Cued Click-Points*(CCP). Rather than five click-points on one image, CCP uses one click-point on each of a sequence of five images.

2. Related Work

Human factors are often considered the weakest link in a computer security system [1]. There are three major areas where human-computer interaction is important: authentication, security operations, and developing secure systems [2]. Authentication is any

protocol or process that permits one entity to establish the identity of another entity [3]. Humans have used three methods for authentication [3]. These methods are:

- Something you know (the password)
- Something you have (credit card, university ID card)
- Something you are (face, voice, signature, fingerprints, DNA, iris)

Today, these methods are called the three factors of authentication [4]. They are

- Token based authentication
- Biometric based authentication
- Knowledge based authentication

Token based techniques such as credit cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security. For example,
ATM cards are generally used together with a PIN number [5]. Tokens have their own weaknesses, however because tokens are simple and cheap to produce, they are also simple and cheap to reproduce. This makes them vulnerable to being counterfeiting. Also, because they are typically a physical object or device, carrying token all the times is inconvenient for users. They can also be stolen more easily than passwords. For this reason, tokens are typically used with another method, such as a PIN code, to reduce their usefulness if stolen [3].

Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security [5].

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords [1].

Text based passwords are not very secure. The problems with text based passwords are:-
1) Passwords should be easy to remember and the user authentication protocol should be executable quickly and easily by humans.
2) Passwords should be secure, i.e., they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text.

Satisfying these requirements is virtually impossible for users. Consequently, users ignore the requirements, leading to poor password practices. This problem has led to innovations to improve passwords. One innovation is graphical passwords, i.e., passwords that are based on images rather than alphanumeric strings. The basic idea is that using images will lead to greater memorability and decrease the tendency to choose insecure passwords.

A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using 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. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage [1].

3. Existing system

The problems of knowledge-based authentication, typically text-based passwords, are well known. Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember.

Text passwords are the most popular user authentication method, but have security and usability problems. Alternatives such as biometric systems and tokens have their own drawbacks. Graphical passwords offer another alternative.

4. Proposed system

The proposed system reduces the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess. This system merges persuasive cued click points and password guessing resistant protocol.

Persuasive Cued Click-Points (PCCP) and conducted user studies evaluating usability and security, provides new evaluation of password distributions, extends security analysis including relevant recent attacks and presents important implementation

details. Results show that PCCP is effective at reducing hotspots (areas of the image where users are more likely to select click-points) and avoiding patterns formed by click-points within a password, while still maintaining usability.

4.1. Click-based graphical passwords

Cued Click Points (CCP) was a new graphical password scheme proposed, wherein user selects one click point on each image rather than multiple click points on single image. During password creation, user has to select the images, sequence of the images and a click point for each image. This data is stored on a server which will be authenticating users as they enter graphical password. At the time of authentication, user has to select the correct click point on each of the images. During authentication, system decides the first image to be displayed. User has to enter click point on the image as images are displayed one after the other on the screen. Click point on each image decides the next image. If the entered click point is correct, the next image displayed will be correct else some random image will be displayed which will not be of the password sequence. Login failure is indicated only after submitting the final click point. Figure 4.1 describes the user login process.

4.2 Persuasive Technology

Persuasive Technology was first articulated by Fogg as using technology to motivate and influence people to behave in a desired manner. He discusses how interface cues can be designed to actively encourage users to perform certain tasks. Forget et al. propose how these may be condensed into a set of core persuasive principles for computer security. 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. The path-of-least resistance for users is to select a stronger password (not comprised entirely of known hotspots or following a predictable pattern). As a result, the system also has the advantage of minimizing the formation of hotspots across users since click points are more randomly distributed.

Our hypotheses were:

1. Users will be less likely to select click- points that fall into known hotspots.

2. The click-point distribution across users will be more randomly dispersed and will not form new hotspots.

3. Users will feel that their passwords are more secure with PCCP. The primary goal of PCCP was to increase the effective password space by guiding users to select more random passwords. To gauge our success, we therefore needed to determine whether PCCP click-points were more randomly distributed across the image and whether they successfully avoided known hotspots from previous studies.

An important usability and security goal in authentication systems is to help users select better passwords and thus increase the effective password space. We believe that users can be persuaded to select stronger passwords through better user interface design. As an example, we designed Persuasive CuedClick-Points (PCCP) and conducted a usability study to evaluate its effectiveness. We obtained favorable results both for usability and security. Graphical passwords provide a useful environment for testing such approaches because it is easier to determine the similarity of passwords and hence test for characteristics such as the occurrence of hotspots.

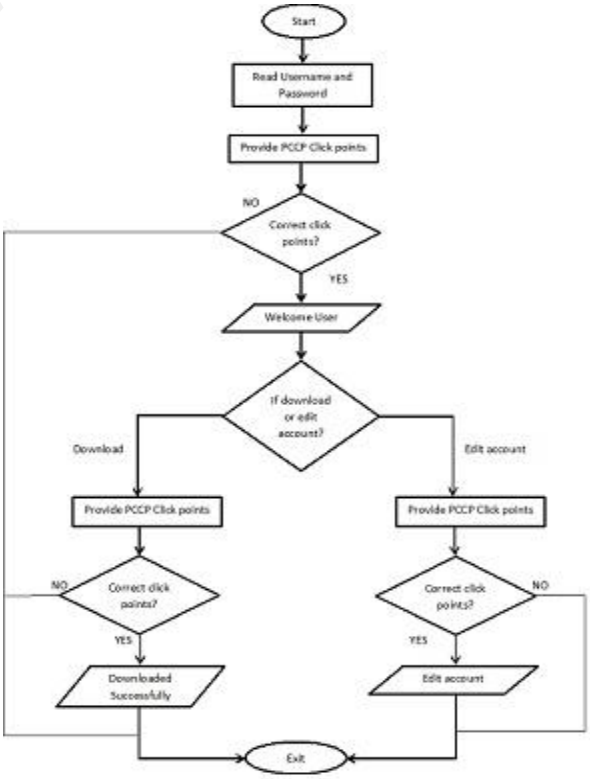

Figure 4.1 User Login Process

5. Results

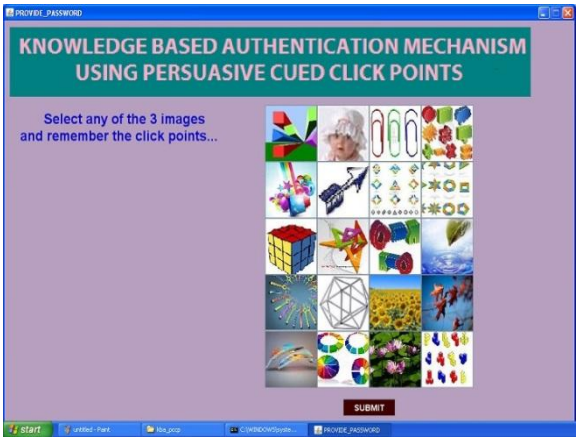

Figure 5.1 Image Selection Process

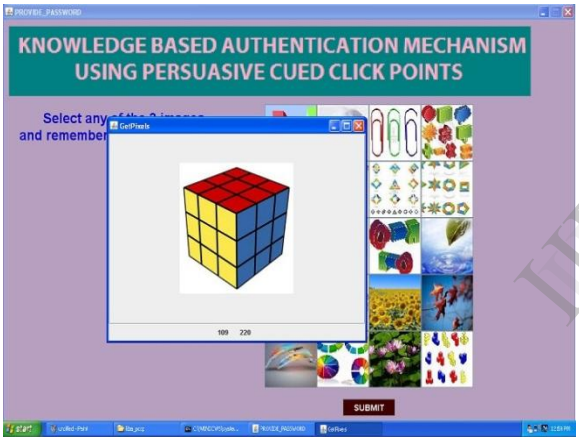

Figure 5.2 Providing PCCP Click Points

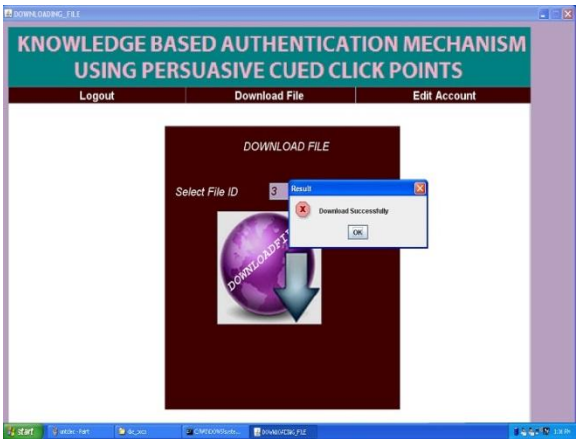

Figure 5.3 File Downloaded Successfully

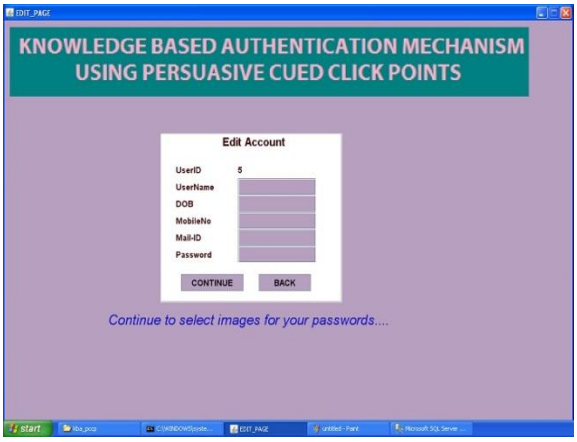

Figure 5.4 Account Editing Process

6. Conclusion

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. The primary goal of PCCP was to increase the effective password space by guiding users to select more random passwords. To gauge our success, we therefore needed to determine whether PCCP click-points were more randomly distributed across the image and whether they successfully avoided known hotspots from previous studies.

This way we would improve security by graphical authentication using PCCP in mobile applications. Well known security threats like brute force attacks and dictionary attacks can be abolished to great extent. This system can be further enhanced by decreasing the size of the tolerance square and also by increasing the number of images.

References

[1] Suo, Xiaoyuan, "A Design and Analysis of Graphical Password" (2006). Computer Science Theses. Paper 27. A. C. L. Andrew S. Patrick, Scott Flinn, "HCI and Security Systems," in CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA, 2003.

[2] "Authentication Methods and Techniques", Christopher Mallow.

[3] "A Graphical Password Based System for Small Mobile Devices", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011, Wazir Zada Khan, Mohammed Y Aalsalem and Yang Xiang.
[4] "Graphical Passwords: A Survey", Xiaoyuan Suo, Ying Zhu, G. Scott, Owen, Department of Computer Science, Georgia State University.
[5] "Enhanced Knowledge Based Authentication Using Iterative Session Parameters", Ali Alkhalifah, Geoff D.Skinner, World Academy of Science, Engineering and Technology 47 2010
[6] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.
[7] A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.
[8] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwest Instruction and Computing Symposium, 2004.
[9] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.
[10] L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002
[11] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.
[12] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996
[13] S. Chiasson, R. Biddle, and P. van Oorschot, "A second look at the usabilty of click-based graphical passwords," in ACM Symposium on Usable Privacy and Security (SOUPS), July2007.