An Authentication System For Information Security Using Cued Click Point And One Time Session Key

Gloriya Mathew, PG Scholar
Department of Computer Science & Engineering, Amal Jyothi College of Engineerng, Kanjirappally

Shiney Thomas, Faculty
Department of Computer Science & Engineering, Amal Jyothi College of Engineering, Kanjirappally

Abstract

User authentication is one of the most important part of information security. Computer security depends largely on passwords to authenticate human users. While there are different types of authentication systems available alphanumeric password is the most commonly used authentication system. But this method has been shown to have significant drawbacks. An alternative solution to the text-based authentication is Graphical User Authentication based on the fact that humans tend to remember images better than text. This type of interface provides an easy to create and remember passwords for the users. However, the issues are shoulder surfing attack which capture the users mouse clicks and image gallery attack that can change the images of the gallery with physical attack. In this paper, we propose a new technique that uses cued click points graphical password method along with the one-time random key for resistance to shoulder surfing attack to make authentication system computationally secure.

1. Introduction

Authentication is the process to allow users to confirm his or her identity to a Web application. Human factors are considered to be the weakest link in a computer security system. There are three major areas where human-computer interaction is important: they are authentication, security operations, and developing secure systems. Here we focus on the authentication problem. A password is a form of secret authentication data that is used to control access to a resource. The password is kept secret from those who are not allowed access, and those who wishing to gain access are tested on whether or not they know the password and are granted or denied access accordingly. The use of passwords goes back to ancient times. They would only allow a person if they knew the password.

In modern times, passwords are used to control access to protected computer operating systems, mobile phones, ATMs machines, etc. A typical computer user may require passwords for many purposes: logging into computer accounts, retrieving email from servers, accessing files, databases, networks, web sites, and even reading the morning newspaper online.

Traditional textual password or PIN, however, relies on keyboard as the input device. Many researchers thereby look at an alternative approach graphical password. Besides the convenience of password input, it is more user friendly in terms of memorability and recallability. The basic hypothesis is that human brain is more capable of storing graphical information than numbers or alphabets; in addition graphical password utilizes an easier and more human friendly memorization strategy recognition based memory, instead of recall based memory for textual password.

In this paper, we proposed a new authentication system which combines the advantages of both graphical passwords and one time session key. The rest of the paper is organized in the following way. In section 2, we provide a brief review of image based passwords and random number key generation. Then, the proposed system implementation is described in section 3. In section 4, compares the proposed system with some prior related work. Section 5 addresses future work and concludes the paper.

2. Overview of the Authentication Methods

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. User authentication is a fundamental component in most computer security contexts. It provides the basis for access control and user accountability. 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. A password authentication system should encourage strong passwords while maintaining memorability. The proposed authentication schemes allow user choice while influencing users towards stronger passwords.

2.1 Authentication Methods

Due to recent events of thefts and terrorism, authentication has become more important for an organization to provide an accurate and reliable means of authentication. Authentication methods are broadly classified into three main areas. Token based (two factor), Biometric based (three factor), and Knowledge based (single factor) authentication.

2.1.1 Token Based Authentication

It is based on "Something You Possess". For example Smart Cards, a drivers license, credit card, a university ID card etc. It allows users to enter their username and password in order to obtain a token which allows them to fetch a specific resource without using their username and password. Once their token has been obtained, the user can offer the token which offers access to a specific resource for a time period to the remote site Many token based authentication systems also use knowledge based techniques to enhance security.

2.1.2 Biometric Based Authentication

Biometric authentication system uses physiological or behavioural characteristics of a person for authentication. It is based on "Something You Are". It uses physiological or behavioural characteristics like fingerprint or facial scans and iris or voice recognition to identify users. A biometric scanning device takes a user's biometric data, such as an iris pattern or fingerprint scan, and converts it into digital information a computer can interpret and verify. A biometric based authentication system may deploy one or more of the biometric technologies: voice recognition, fingerprints, face recognition, iris scan, infrared facial and hand vein thermo grams, retinal scan, hand and finger geometry, signature and keystroke dynamics. Biometric identification depends on computer algorithms to make a yes/no decision. It enhances user service by providing quick and easy identification.

2.1.3 Knowledge Based Authentication

Knowledge based techniques are the most extensively used authentication techniques and it include both text based and picture based passwords. Knowledge based authentication (KBA) is based on "Something You Know" to identify you For Example a Personal Identification Number (PIN), password or passphrase. It is an authentication scheme in which the user is asked to answer at least one "secret" question. KBA is often used as a component in multifactor authentication (MFA) and for self service password retrieval. Knowledge based authentication (KBA) offers several advantages to traditional (conventional) forms of authentication like passwords, PKI and biometrics.

2.2 Image based Password

Image based password (graphical password) refers to using pictures as passwords. Graphical password have been proposed as a possible alternative to text based, motivated particularly by the fact that humans can remember pictures better than text. Visual objects seem to offer a much larger set of usable passwords. Psychological studies have shown that people can remember pictures better than text; especially photos, which are even easier to be remembered than random pictures. For example we can recognize the people we know from thousands of faces; this fact was used to implement an authentication system. Also, they should be more resistant to brute force attacks, since the search space is practically infinite. To improve the security, a user could choose a sequence of points in an image as a password; this leads to a vast number of possibilities, if the image is large and complex, and if it has good resolution. This is the basis for the graphical passwords. An excellent survey of the numerous graphical password schemes has been developed. In general, graphical passwords techniques are classified into two main categories:

- Recognition based techniques
- Recall based techniques
- Cued recall based techniques

In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images (e.g., faces, random art images, images clustered into semantic categories) he or she chooses during the registration stage. This procedure can be repeated for a number of rounds to increase the password space. In recall based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Passfaces is a recognition- based technique, where a user is authenticated by challenging him/her into recognizing human faces. An early recall-based graphical password approach was introduced by Greg Blonder where a user can apply of a series of clicks on predefined regions of an image. Later, Wiedenbeck proposed Passpoints, wherein passwords could be composed of several points anywhere on an image.

2.3 Cued Recall based technique

Graphical password systems are a type of knowledge based authentication that attempts to leverage the human memory for visual information. A comprehensive review of graphical passwords is available elsewhere. Of interest herein are cued recall click based graphical passwords (also known as locimetric). In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues to aid recall.

Example systems:

- Passpoints
- Cued-click points

2.3.1 Passpoints

In Passpoints, passwords consist of a sequence of 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, within a system defined tolerance square of the original click points Although Passpoints is relatively usable, security weaknesses make passwords easier for attackers to predict. Hotspots are areas of the image that have higher likelihood of being selected by users as password click points. Attackers who gain knowledge of these hotspots through harvesting sample passwords can build attack dictionaries and more successfully guess Passpoints passwords. Users also tend to select their click points in predictable patterns (e.g., straight lines), which can also be exploited by attackers even without knowledge of the background image; indeed, purely automated attacks against Passpoints based on image processing techniques and spatial patterns are a threat.

2.3.2 Cued Click Points

Cued Click Points was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Rather than five click points on one image, CCP uses one click-point on five different images shown in sequence. The next image displayed is based on the location of the previously entered click point, creating a path through an image set. Users select their images only to the extent that their click point determines the next image. Creating a new password with different click point's results in a different image sequence. The claimed advantages are that password entry becomes a true cued-recall scenario, wherein each image triggers the memory of a corresponding click point. Remembering the order of the click points is no longer a requirement on users, as the system presents the images one at a time. CCP also provides implicit feedback claimed to be useful only to legitimate users. When logging on, seeing an image they do not recognize alerts users that their previous click point was incorrect and users may restart password entry. Explicit indication of authentication failure is only provided after the final click point, to protect against incremental guessing attacks.

2.4 One-Time Password

A one-time password (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid. On the downside, OTPs are difficult for human beings to memorize. Therefore they require additional technology to work. In the proposed system a random number OTP is generated by the system during each login session and is send to the users mobile using a GSM modem.

3. Proposed System

The proposed system is a combination of graphical password and a one-time session key. The system allows the user to select three image passwords one in each level. When the user uploads the image password, the system will divide the uploaded image into a 3x3 grids. The system will provide four options (status) for labelling the grids. The four options are: Left to Right, Right to Left, Top

to Bottom and Bottom to Top. The user can choose any of these options for each of the image password. The user must have to remember the image password & status that he chooses as each image password during login stage. A random number session key (One Time Password-OTP) is generated by the system and send to users mobile for login to the system. The OTP consists of three random numbers which indicates the grid to be clicked on image password in each level of login stage.

The proposed authentication system works as follows: At the time of registration, after filling the signup form, the user creates a graphical password by first uploading a picture he or she chooses from his own system using "UploadImage1" button. The user then chooses any one status from given four options: Left-right, Right-Left, Top-bottom, and Bottom-top. The system will then divide the selected picture into a 3x3 grid and label each grid according to the selected status. When the user click on the "Next" button the window for creating image password level-2 is displayed. In this window user have to click on to the "UploadImage2" button to select the second picture as next image password. After selecting the picture the user must have to choose the option for labelling the grids in the picture. Then user click on to the "Next" button once more to select the third picture (image password) as in the previous levels. Finally click on the "Finish" button to complete the registration phase. Figure 1 shows a screenshot for creating image password in registration phase.

For authentication the user first enters his userid. Then click on the "Next" button. At the same time a onetime random number key is issued by the system to the user's mobile number given at the registration stage. For example suppose key is 386. Now the system

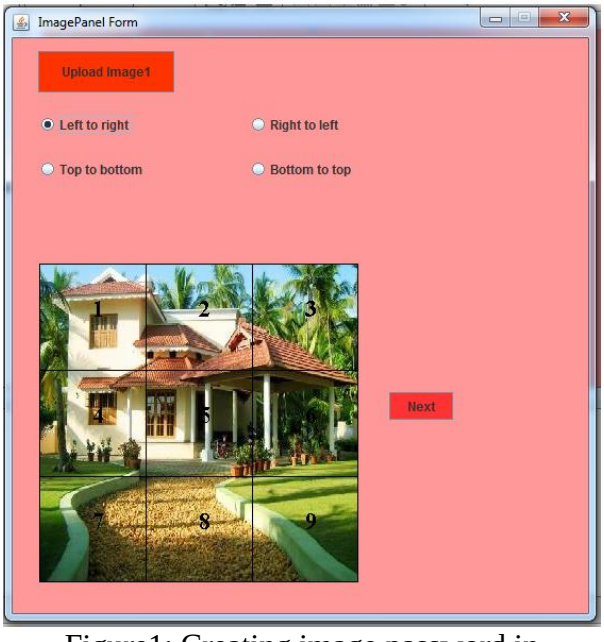

Figure1: Creating image password in registration phase

displays four images which is not labelled. One among this is the first image uploaded by the user and rest of the three images are extra images displayed by the system for confusioning the hacker. Since the key is 386, the user must have to click on the grid 3 on the actual picture among the four images. Then click on "Next" button. Now another set of four images is displayed. Among these four images one will be the second image uploaded by the user during the registration stage and the other three images will be displayed by the system for protecting from hacker. From these four images the user have to correctly click on the grid 8 in the second image uploaded by him. Similarly, when we click on "Next" button another set of four images is displayed. Among these four images one will be the third image uploaded by the user and three images will be displayed by the system. The user must have to correctly click on the grid 5 according to the grid labelling option given to this image during the registration phase. If all the clicks in each level of images are correct then user can successfully logon to the

system. Otherwise if there is any mistake in any of the click point(grid no.) system will displays an error message to the user. Figure 2, shows the screenshot of the login screen.

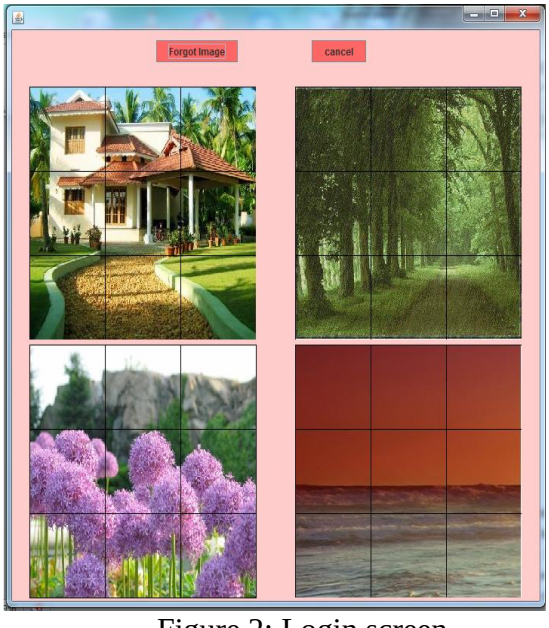

Figure 2: Login screen

4. Security Analysis

The inclusion of one time password along with cued click based graphical password method has improved the system performance to a great extent. It has an added advantage of the One-time session key and cued click point authentication systems. There is no possible method to break the system using cameras, key loggers and mouse detection software's. The proposed system will overcome hotspot problem seen in many of the graphical password authentication systems. Table 1 shows the security features of different graphical password based systems.

5. Conclusion

Graphical passwords are strong alternatives to text based and biometric authentications. It is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack, etc. User authentication is a fundamental component in most computer security contexts. In this paper, we proposed a secure graphical password authentication system. The system combines graphical and onetime session key trying to achieve the best of both methods

System	Features based on.						
	Text	Graphical	AOI	Order sensitivity	sensitivity	Session Key	Possible attacks
Passface	-	✓	✓	-	-	-	Dictionary attack, Brute force attack, Shoulder surfing.
Blonder's scheme	-	✓	✓	-	-	-	Dictionary attack, Brute force attack, Shoulder surfing.
Weidenbeck et.al.	-	✓	✓	✓	-	-	Dictionary attack, Brute force attack, Shoulder surfing.
A Graphical Password authentication system	✓	✓	-	✓	✓	✓	Capture attack
Proposed System	✓	✓	✓	✓	✓	✓	-

Table1: Comparison of security features of various graphical password systems

which will increases the security. Since a random number security key is generated in each login stage the key cannot be used again and it will enhances the security of the system. The proposed system can be used in

desktop locking applications, network security as well as web security.

References

- Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism Sonia Chiasson, Member, IEEE, Elizabeth Stobert, Student Member, IEEE, Alain Forget, Robert Biddle, Member, IEEE, and Paul C. van Oorschot, Member, IEEE.
- Network Security-Overcome Password Hacking Through Graphical Password Authentication M. Arun Prakash, T. R. Gokul.
- 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.
- Alain Forget, Sonia Chiasson, P. C.van Oorschot, Robert Biddle Improving Text Passwords Through Persuasion.
- XiaoyuanSuo, Ying Zhu, and G. Scott Owen. Graphical passwords: A survey. In Proceedings of Annual Computer Security Applications Conference
- S. Chiasson, R. Biddle, and P. van Oorschot(2012) . A Second Look at the Usability of Click-Based Graphical Passwords“ Proc. ACM Symp. Usable Privacy and Security (SOUPS).
- Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. Passpoints: design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies.