GRAPHICAL USER AUTHENTICATION SYSTEM (GUAS)

TAN WOEI WEN

THESIS SUBMITTED IN FULFILMENT OF THE DEGREE OF COMPUTER SCIENCE

FACULTY OF COMPUTER SYSTEM AND SOFTWARE ENGINEERING

2014

Abstract

Nowadays, the most accepted computer authentication technique is to use alphanumerical usernames with text-based password. This method has been proven to have significant multiple weaknesses. For example, users tend to choose the passwords that can be easily cracked. On the other hand, if a password is difficult to guess, then it is often hard to memorize. To address those issues, some researchers have developed graphical-based authentication algorithm that implement pictures as passwords. In this project, I had conduct an in-depth comprehensive review regarding the existing graphical password scheme. Furthermore, I classify these existing Graphical User Authentication System (GUAS) into two kinds of mechanism, which are: recognition-based and recall-based approaches. Besides that, I will examine the strengths and limitations of each technique and identify the future research directions. I also developed an improved version of GUAS algorithm address the common limitation exists in the current graphical password techniques. Overall, in this thesis, the scheme of the new technique will be proposed, the advantages of technique will be outlined and lastly, the future work will be anticipated as well.

ABSTRAK

Pada masa kini, teknik pengesahan pengguna komputer yang paling diterima oleh masyarakat adalah menggunakan kata laluan berasaskan teks. Kaedah ini telah dibuktikan mempunyai pelbagai kelemahan yang ketara. Sebagai contoh, pengguna cenderung untuk memilih kata laluan yang mudah diteka. Sebaliknya , jika kata laluan yang sukar untuk diteka , maka ia sering sukar untuk dihafal oleh pengguna. Bagi menangani isu-isu ini, beberapa penyelidik telah berlahirkan teknik pengesahan dengan berdasarkan bantuan grafikal seperti, mengguna gambar sebagai kata laluan. Dalam projek ini , saya akan menjalankan kajian semula yang mendalam dan komprehensif mengenai skim kata laluan grafik yang sedia ada. Tambahan pula, saya telah mengelaskan teknik pengesahan grafikal kepada dua jenis mekanism. Selain itu, saya akan mengkaji kekuatan dan batasan setiap teknik serta mengenal pasti arah penyelidikan masa depan. Saya juga membangunkan satu teknik pengesahan grafikal yang lebih baik dan dapat menyelesaikan isu-isu wujud dalam teknik kata laluan grafik semasa ini. Dalam tesis ini, skim teknik baru akan dicadangkan, kelebihan teknik akan dibincang, akhir sekali, kerja masa depan akan dijangka juga.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1 INTRODUCTION

1.1 Project Overview

Indeed, the internet and the usage of computer are rising up rapidly.

More and more aspects of human life are moving to online nowadays. The internet is a global network connecting of billions computer to exchanges of data, news and opinions. Obviously, vast range of human activities is depending on internet, including online banking transaction, online merchandize/shopping and online research.

Furthermore, peoples also using the Internet as their main social tools as well. Undoubtedly, in the last few years there is been an impressive growth in the number of social networking sites such as Facebook. Peoples often tend to share many kinds of their personal information on the social networking website as well as their name, recent status, their current location and etc. Hence, It is essential for us both as internet users and as educated man to continually think about the issues had been arise from internet technology.

With the amount of online identify theft and hackers currently prowling on the internet, it is very crucial to fully protect our computer from online dangers. This is important for every one of us, not just the overly security conscious. Foremost, the very first line of defense on the web is using the password. Passwords able to ensure the confidentiality and security of data which are stored on various workstations and prevent our online account exposed to the identity theft easily. Ultimately, the usage of password will decrease the risk of internet user to become a victim of cybercrime

The most usual computer authentication method is to implement the alphanumerical password for account or system login session. But, this method has been proven to have some significant drawbacks. For example, users tend to choose the passwords which can be easily hacked or guessed. On the other hand, if a password is strong enough, then it is always difficult to memorize it. To address this problem, some IT researchers have developed many kind of alternative authentication methods that based on the usage of image as passwords or the combination of picture and alphanumerical method.

Even though the graphical user authentication system (GUAS) is able to counter some of the drawback of the alphanumerical method, yet the strengths and limitations of each graphical method are still remain disputable such as implementation issues and major design weakness for the graphical password. Thus, this project will aim to discuss the usability of the current available GUAS and propose an improved version of graphical user authentication techniques against the commonly seeing problems in the graphical password area nowadays.

1.2 Problem Statement

Current available authentication systems are suffered from many kinds of weaknesses and limitation. The vulnerabilities of the text-based password scheme have been well known. Users always tend to choose short-length passwords or passwords which are easy to memorize, hence, this situation makes the passwords susceptible to password crackers or hackers. Furthermore, text-based password in alphanumerical scheme is vulnerable to dictionary attack, brutal guessing, social engineering, key-loggers, hidden-camera,spyware attacks, shoulder surfing and etc.

To address the limitations of text-based password, techniques such graphical-based password have been put in use. Other than that, additional input devices such as mouse, stylus and touch-screen that permit have raised the usability of the graphical user authentication techniques. The primary objective of enhancing the current user authentication scheme is to strengthen the method in the aspect of security and usability. Graphical password schemes have been proposed as a possible alternative to text-based schemes which motivated by the fact that humans can recognize graphical images better than text. In additional, psychological studies have shown that pictures are generally easier to be memorized or recognized than text. However, they are still mostly vulnerable to shoulder-surfing as well.

Shoulder-surfing attack is a direct observation technique, such as peeking over someone's shoulder (casual eavesdropping) to sneak their sensitive personal information. For instance, when a user enters information or password using a mouse, keyboard, touch screen or any conventional input device, a malicious observer may be able to acquire the user's password easily by watching in the user's vicinity. This is a problem that has been difficult to overcome even for the current GUAS scheme.

Previous research has proven that a graphical password is more memorable than a strong (non-dictionary term) alphanumeric passwords. On the others hand, participants in a prior study expressed concerns that the improvement of memorability necessarily leads to higher risks of shoulder-surfing. Another potential drawback with graphical passwords is that it takes longer to input graphical passwords than textual passwords. The login process is slow and it may frustrate the impatient users. These entire limitations appear to be yet another classic example of the common trade-off between security and usability for a user authentication system.

For this project, I will first conduct a comprehensive outline of the existing graphical user authentication systems. Furthermore, a deeper discusses of the strengths and limitations of each method will be carrying out. Ultimately, this project will proposed an improved version of graphical password scheme which has desirable usability and better security feature by combination of the current available GUAS (hybrid of GUAS).

1.3 Background

One of the primary functions of any security system is to manage the movement of people to the protected areas, such as physical buildings, national borders or even our information systems. In fact, the systems data and the information those commit to computer memory or store on internet mostly are valuable resources which need to be protected. The first line of defense to repel the cybercriminal from ours crucial information is creating a password to authenticate the identity of user.

Typically, conventional password is composing of a string of letters and digits, i.e. alphanumeric. Passwords are simply secrets that shared by the verifier and the system user. Besides that, the passwords are in an encrypted form when stored on a server so that an invasion of the file system does not necessary will expose the password lists. Yet, such passwords have the drawback of being hard to remember. While weak passwords are often susceptible to dictionary attacks and brute force attacks where as strong passwords are difficult to memorize.

To resolve the problems associated with text-based authentication systems, the researchers have proposed the concept of GUAS and constructed alternative authentication mechanisms. GUAS is the most promising alternative to the conventional text-based password authentication systems. GUAS utilize the usage of images instead of textual passwords and are particularly motivated by the reality that humans can memorize graphical object more efficient than a string of characters. Thus, GUAS provide a measure for a more user-friendly password authentication session while able to enhance the level of security.

Just like humans, there is no perfect technology existed, hence, there will be type of flaw or limitation for the GUAS scheme as well. But, as an organism could using own minds in autonomous and creative manners, we should explore our limits and ask for what is not obvious. Ultimately, we are able propose and evaluate a new GUAS scheme which has a desirable usability with ideal security level.

1.4 Aim of the Project

The objectives of this project are:-

1. To discuss and analyze the current existing GUAS in term of security, usability and reliability features.
2. To propose an improved version of GUAS method that able to achieve balance between the aspect of security, usability and reliability.

1.5 Project Scope

1. Develop a user authentication system based on graphical scheme.
2. Proposing an improved GUAS algorithm while balance the trade-off between level of security, usability and reliability.

1.6 Thesis Organizations

This thesis consists of six main chapters. Chapter 1 will provide some brief overview on the introduction of the project. In this chapter, we can identify the need of a reliable alternative user authentication system is crucial due to the rampant cybercriminal and information security issues nowadays. Chapter 1 will expose the fact that GUAS had facing some limitation and drawback as well. Lastly, this chapter will cover the main objectives, scope of project and the overall thesis organizations.

In Chapter 2, it will contain the literature review of the project. We will first conduct a discussion of the several well-known and frequently used GUASs. Furthermore, the analysis of the strengths and limitations of each method will be undergone, hence, point out the future research directions in this area. Recommendations and opinion will be given based on the GUAS scheme as well on this chapter.

Chapter 3 will describes about the detail of methodology use for this project. Thus, we are able to explore on selected methodology and the steps used to establish this project. Furthermore, we will also be defining the requirement on which technique or tools are utilized when conducting the project. In addition, we will be discussing on which software and hardware is applied for carry out the development of this project. The Gantt chart is available to be review on this chapter as well.

Hence, in chapter 4 we propose the development of the framework and model through flow work. It will reveal the process and data gathering for research purposes, thus, sketching the work flow and model. We will also suggest on how the data or model has been implemented into the selected algorithm. Furthermore, we will be approach to the process that involved during the development of this project. The test and result will presented using the statistical tools accordingly.

Chapter 5 generalized the explanations about the findings and the results from data analysis. We also evaluated on the analysis result that related with the project aims and objectives. Through the chapter, the statement of constraint met and trade-off between security and efficiency during development of project will be exposed. Discussion about the suggestion and space of improvement in order to secure utilization for the future development of this project will be provided on this chapter as well.

For the last chapter, chapter 6 will summarize the findings throughout of the project. Finally, the implication of the future enhancement and project constraint will be discussed to conclude the project.

1.7 Summary

As a conclusion, for this chapter we have explored the overview on the introduction of the project. Besides that, we also identified the need of a reliable alternative user authentication system is crucial due to the rampant cybercriminal and information security issues nowadays. Furthermore, we had point out the aim of the project as our future research directions. Lastly, this chapter has outlined the scope of project and the overall thesis organizations as well.

CHAPTER 2 LITERATURE REVIEW

2.1 Introduction

For the security sensitive environments, it is crucial to safeguard the resources against unauthorized access at all cost such as enforcing the access control mechanisms. Hence, authentication session plays an important part in protecting resources against unauthorized malicious use. Tons of authentication methods exist in our environment nowadays, from simple password text-based authentication system to the costly and computation profound biometric authentication systems. Basically, current existing user authentication scheme can be branches into three fundamental fields:

- Token based authentication
- Biometric based authentication
- Knowledge based authentication
    - ✓ Text based
    - ✓ Graphic based

Token based techniques, such as tag cards, ATM cards and key cards are broadly used. Several token-based authentication systems also applied with knowledge based techniques to amplify the security level. For instance, ATM cards are usually used together with the PIN number.

For the biometric based authentication techniques, it consists of a few methods, such as, iris scanning, fingerprints authentication or facial recognition, but they are not yet widely adopted by the society. The major drawback of the biometric approach is that such systems can be over-costly, and the identification procedure can be time-consuming and often unreliable. Nevertheless, this sort of method presents the uppermost level of security.

Knowledge based techniques are the most popular authentication techniques in this century and it include of text-based and graphic-based authentication method. The most common knowledge text-based authentication approach is for a user to comply a user name and a text-based password. The vulnerabilities of this technique have been well known. One of the main worriment is the difficulty of memorizing the passwords. On the others hand, the graphic-based scheme can be further divided into two groups: recognition-based and recall-based graphical techniques. Implement the recognition-based techniques, firstly, a user will be presented with a set of images and the user must get through the authentication by identifying and recognizing the images he or she pre-selected during the registration phase. However, recall-based techniques require a user to regenerate something that he or she created or previously chosen during the registration phase. For this chapter, we will have a depth analysis on the existing current GUAS and discuss in term of their limitation as well as the advantages respectively.

2.2 Recognition-based Techniques

The basic idea of this method is a user will be presented with a set of images and the user must get through the authentication by identifying and recognizing the images he or she pre-selected during the registration phase.

2.2.1 D´ej`a Vu

Dhamija and Perrig developed a graphical authentication scheme based on hash visualization technique.

"We develop a prototype of D´ej`a Vu and conduct a user study that compares it to traditional password and PIN authentication. Our user study shows that 90% of all participants succeeded in the authentication tests using D´ej`a Vu while only about 70% succeeded using passwords and PINS. Our findings indicate that D´ej`a Vu has potential applications, especially where text input is hard (e.g., PDAs or ATMs), or in situations where passwords are infrequently used (e.g., web site passwords). (R. Dhamija and A.

Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.)"

In the Deja Vu system, user will be asked to choose particular number of picture from a set of random images provided by a program. Later, user will be required to recognize the pre-selected pass-images in order to be authenticated. The results showed that almost 90% of all participants succeeded in the authentication session while using their technique, while only 70% successful accomplish using text-based passwords and Pins. However, the average time to complete the process is longer than the conventional approach, but has a much lesser failure rate. A drawback is that the server is required to store a huge amount of graphical material which may have to be transferred over the network, hence, delaying the authentication procedure. Another limitation of this system is that the server also needs to store the seeds of the portfolio images of each user in plain text. In term of interface, the process of selecting a picture from picture database can be time consuming and tedious for the user.

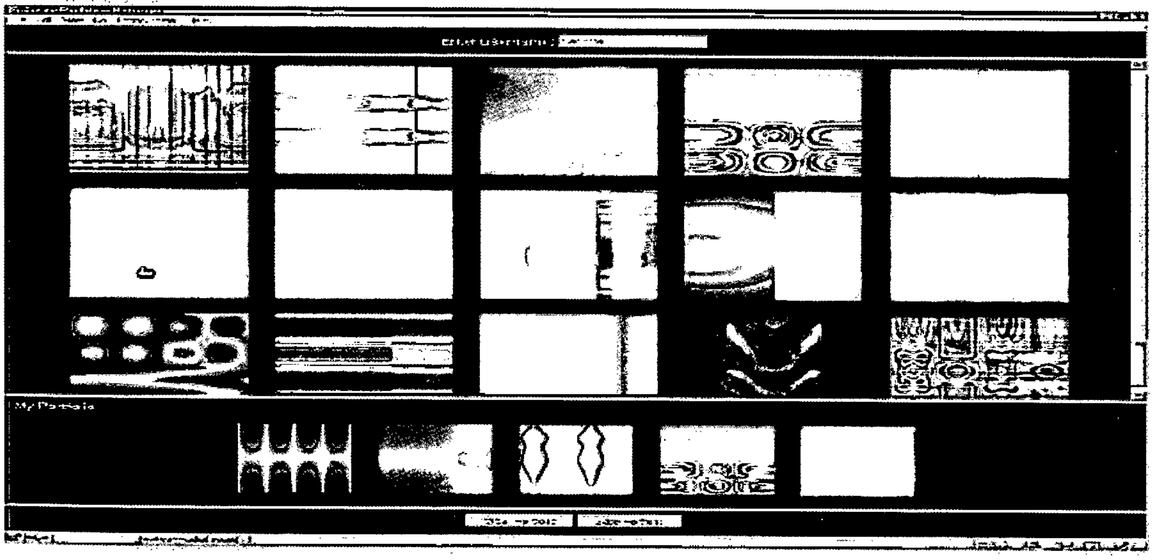

Figure 1: Example of random art images.

In Akula and Devisetty's algorithm, the system displays batch of images to the user and the user would then choose their pass-image to authenticate themselves to the server. Generally, the basic scheme of this method is identical to the technique proposed by Dhamija and Perrig.

"The system does not store the images. The images are read byte wise and hashed using a secure hashing function SHA-1. Images are large files. But SHA-1 algorithm produces a 20 byte output which is very secure and requires less memory. This system was implemented in Java. Java is platform independent, portable and most suitable for Internet applications. (S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwest Instruction and Computing Symposium, 2004.) "

On the contrary, the difference is that this technique implements the hash function SHA-1, which produces a 20 byte output. This ensures the authentication to be more secure and requires less memory. However, image files still tempt to occupy more space than normal text file even after hashing. For this reason, Akula and Devisetty had suggested a possible future enhancement by providing the persistent storage and this could be integrated on the Internet, cell phones or PDA's.

2.2.2 Sobrado and Birget Algorithm

Sobrado and Birget proposed a graphical password technique that able to deal with shoulder-surfing limitation. At first, the system will show a few of pass objects (pre-selected by user) among many other decoy objects. The user is required to recognize pass-objects and clicking inside the area of convex hull which formed by the pass objects.

"The system randomly scatters a set of N objects on the screen. In practice, the number N could be a few hundred or a few thousand, and the objects should be different enough so that the user can distinguish them. In addition, there is a subset of K pass-objects (e.g., K = 10) previously chosen and memorized by the user. At login the system will randomly choose a placement of the N objects. However, the system first randomly chooses

a patch that covers half the screen, and randomly places the K chosen objects in that patch. To login, the user must find 3 of the pass-objects and click inside the invisible triangle created by those 3 objects. This is equivalent to saying that the user must click inside the convex hull of the pass-objects that are displayed. In addition, for each login this challenge is repeated a few (e.g., 10) times using a different display of some of the N objects. Therefore, the probability of randomly clicking in the correct region in each challenge is very low.(L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.)"

In order to strengthen the password and make it hard to predict, Sobrado and Birget recommended using 1000 objects, which making the display very complicated and the objects almost indistinguishable. Besides that, using fewer decoy objects may lead to a smaller password space due to the resulting convex hull can be huge. In their second algorithm, a user is order to move a frame (contain the one of the pass objects within it) until the pass object on the frame lines up and meet with the other pass-objects. In additional, the authors advise the authentication session should repeat the process for a few more times to diminish the likelihood of logging in by randomly rotating or clicking. The main limitation of these algorithms is that the procedure can be very time consuming and frustrated the user.

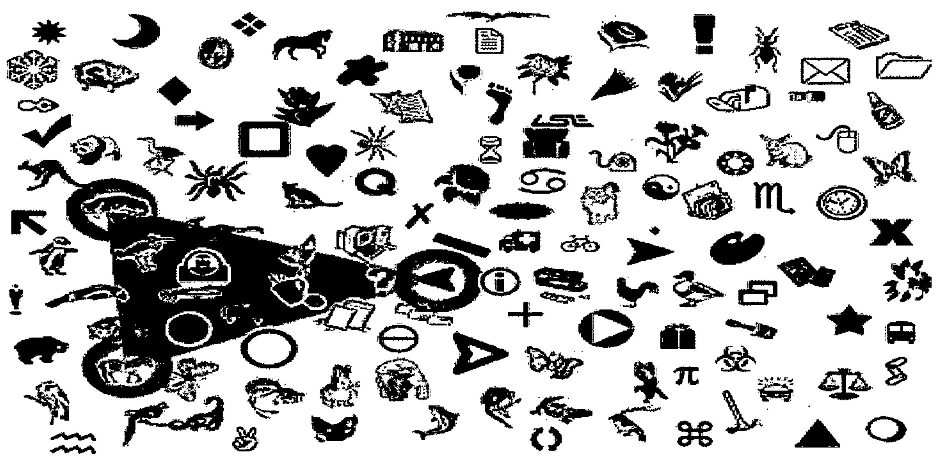

Figure 2: Sobrado and Birget first algorithm.

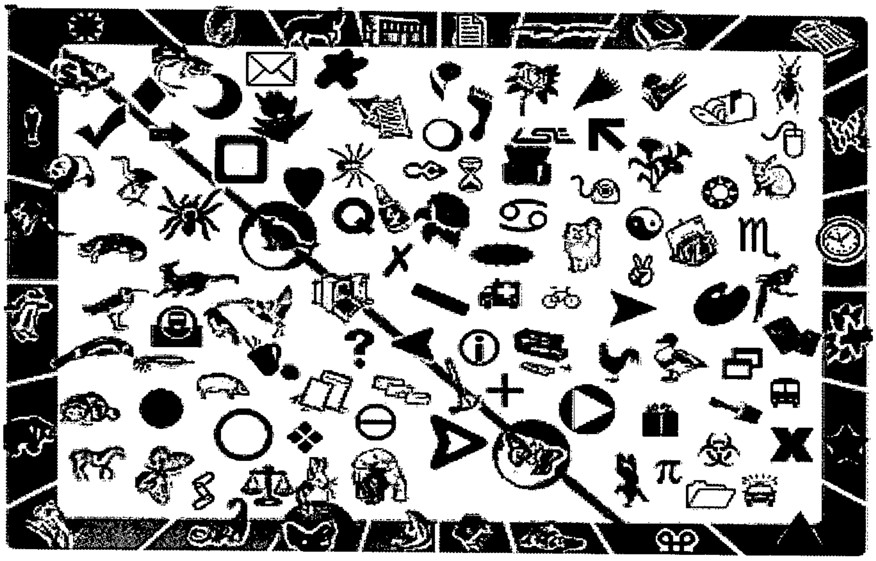

Figure 3: Sobrado and Birget second algorithm.

2.2.3 Man,et al Algorithm

Man, et al. had proposed another shoulder-surfing resistant algorithm.

"We propose a password scheme. This scheme is obtained by adding light graphic layer to the traditional text-based password scheme. In this graphic layer, we randomly generate patterns of icons which are easy for user who owns the password to recognize and difficult for a shoulder-surfing attacker to find out. (S. Man, D. Hong, and M. Mathews, "A shoulder-surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003.)"

In this algorithm, a user asked to choose a few of image as pass-objects. Each pass-object consist several variants and each variation is designated a unique text-based code. During the authentication, user is confronted with several scenes. Each scene consists of several pass-objects (each in the form of a randomly picked variant) and many decoy objects. The user has to insert a string contain the unique codes matching to the pass-object variants introduce in the scene as well as a code expressing the relative location of the pass-objects. The argument is that it is very difficult to crack or guess this kind of password