DYNAMIC ANALYSIS ON PIXEL VALUE GRAPHICAL PASSWORD SCHEME

MOHD SIDEK FADHIL BIN MOHD YUNUS

Thesis Submitted to the Centre for Graduate Studies, Universiti Pertahanan Nasional Malaysia, in Fulfillment of the Requirements for the Degree of Master of Science (Computer Science)

December 2014

ABSTRACT

For decades, authentication system relied on username and password as pass-phrase object for the authentication process. The longer, wider the variety of symbol choices, and randomly arranged phrase considered as a strong password. A strong password is hard to memorise and makes it less preferred by most of the users in most of the cases. Psychological study that shows human is better at recognising and remembering images. Therefore, graphical password mechanism was introduced to reduce human memory burden. There were two types of graphical password introduced for the past twelve years which are click-based and draw-based graphical password scheme. Click-based graphical password scheme requires users to recognise and click in sequence during authentication. Draw-based graphical password scheme requires user to memorise pattern during authentication. However, draw-based graphical password scheme requires specific drawing input device makes it less preferable to implement that click-based graphical password scheme. Meanwhile, click-based graphical password scheme is vulnerable to shoulder surfing and click attempt because of exposed clickable pass-object on authentication interface. Based on literature analysis of click-based graphical password scheme limitations has lead to the design features and criteria for pixel value graphical password scheme. Pixel value graphical password scheme was designed to meet the identified features and criteria that overcomes click-based graphical password scheme limitations. By removing exposed and clickable pass-object features on graphical password, pass-object cannot be seen by other users and requires large attempt effort to break. Compliance analysis on graphical password scheme shows that it is fit to overcome limitations of click-based graphical password scheme. Therefore, pixel value graphical password scheme users may use their most meaningful image as pass-object to make pass-object more memorable in secure way and less risk.

ABSTRAK

Dalam beberapa dekad, sistem autentikasi bergantung kepada pengunaan nama pengguna dan kata laluan sebagai objek frasa laluan untuk proses pengesahan. Susunan aksara yang kompleks, lebih panjang, penggunaan simbol lebih luas, dan susunan frasa secara rawak dianggap sebagai kata laluan yang kuat. Kata laluan yang kuat adalah sukar untuk diingati dan membuatkannya kurang dipraktikkan dalam kebanyakan kes oleh sebahagian besar pengguna. Mekanisme kata laluan grafik diperkenalkan untuk mengurangkan beban ingatan manusia di mana kajian psikologi menunjukkan manusia lebih baik mengenali dan mengingati gambar. Terdapat dua jenis kata laluan grafik diperkenalkan sepanjang dua belas tahun yang lepas iaitu skim kata laluan grafik kaedah klik dan kaedah lukisan corak. Kaedah klik memerlukan pengguna untuk mengenali titik klik dan klik mengikut urutan semasa pengesahan. Kaedah lukisan corak pula memerlukan pengguna untuk melukis semula corak semasa pengesahan. Walau bagaimanapun, skim kata laluan grafik kaedah lukisan memerlukan peranti input lukisan yang khusus membuatkannya kurang diaplikasi berbanding kaedah klik. Dalam masa yang sama, skim kata laluan grafik kaedah klik pula terdedah kepada serangan *shoulder surfing* dan cubaan klik kerana objek laluan di muka pengesahan terdedah dan boleh diklik. Berdasarkan analisa literasi ke atas batasan-batasan skim kata laluan grafik kaedah klik telah membawa kepada penghasilan cirri-ciri dan kriteria reka bentuk untuk skim kata laluan grafik berasaskan nilai piksel. Dengan menghapuskan ciri-ciri objek laluan yang terdedah dan boleh diklik, objek laluan tidak boleh dilihat oleh pengguna lain dan memerlukan usaha yang lebih besar untuk dipecahkan. Analisa pematuhan pada skim kata laluan grafik menunjukkan bahawa ia sesuai untuk mengatasi keterbatasan skim kata laluan grafik kaedah klik. Oleh itu, pengguna skim kata laluan grafik berasaskan nilai piksel boleh menggunakan gambar yang sangat bermakna pada mereka sebagai objek laluan dalam cara yang selamat dan berisiko rendah.

ACKNOWLEDGEMENT

My infinite gratitude to Allah Subhanahu Wa Ta'ala for kindly awarding me strength to accomplish my study on pixel value graphical password scheme through more than two years research work.

I am infinitely indebted to my parents for supporting and encouraging me for these past few years. Without their kindness, I will not be willing to accomplish this research.

I would also like to address my greatest thank you to my research supervisor, Dr. Mohd Afizi Bin Mohd Shukran, for his guidance and support while completing this research.

My special thanks to lecturers of FSTP and my friends for their help and support.

Thank You.

APPROVAL

I certify that an Examination Committee has met on **30 MAY 2014** to conduct the final examination of **MOHD SIDEK FADHIL BIN MOHD YUNUS** on his degree thesis entitled **DYNAMIC ANALYSIS ON PIXEL VALUE GRAPHICAL PASSWORD SCHEME**. The committee recommends that the student be awarded the **MASTER OF SCIENCE (COMPUTER SCIENCE)**

Members of the Examination Committee were as follows.

ABDUL GHAPOR BIN HUSSIN, PhD
Professor
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Examination Chairman)

OMAR BIN ZAKARIA, PhD
Associate Professor
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Internal Examiner)

RABIAH BINTI AHMAD, PhD
Associate Professor
Department of System & Computer Communication
Universiti Teknikal Melaka (UTEM)
(External Examiner)

APPROVAL

This thesis was submitted to the Senate of Universiti Pertahanan Nasional Malaysia and has been accepted as fulfillment of the requirements for the degree of **Master of Science (Computer Science)**. The members of Supervisory Committee were as follows.

MOHD AFIZI BIN MOHD SHUKRAN, PhD
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Main Supervisor)

KAMARUZAMAN BIN MASKAT
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Co-Supervisor)

UNIVERSITI PERTAHANAN NASIONAL MALAYSIA

DECLARATION OF THESIS

Author's full name : **MOHD SIDEK FADHIL BIN MOHD YUNUS**
Date of Birth : **6th OCTOBER 1986**
Title : **DYNAMIC ANALYSIS ON PIXEL VALUE GRAPHICAL PASSWORD SCHEME**
Academic session : **FEBRUARY 2012**

I declare that this thesis is classified as:

□ **CONFIDENTIAL** (Contains confidential information under the Official Secret Act 1972)

□ **RESTRICTED** (Contains restricted information as specified by the organization where research was done)

☑ **OPEN ACCESS** I agree that my thesis to be published as on-lines open access (full text)

I acknowledge that Universiti Pertahanan Nasional Malaysia reserves the right as follows.

1. The thesis is the property of Universiti Pertahanan Nasional Malaysia.
2. The library of Universiti Pertahanan Nasional Malaysia has the right to make copies for the purpose of research only.
3. The library has the right to make copies for academic exchange.

861006-23-6271	MOHD AFIZI BIN MOHD SHUKRAN, PhD
Date:	Date:

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

DAS	: Draw a Secret
DCT	: Discrete Cosine Transform
DNA	: Deoxyribose Nucleic Acid
DST	: Discrete Sine Transform
EFT	: Electronic Fund Transfer
GIF	: Graphic Interchange Format
GUI	: Graphical User Interface
HTTP	: Hyper Text Transfer Protocol
IDCT	: Inverse Discrete Cosine Transform
IEC	: International Electrotechnical Commission
IP	: Internet Protocol
ISO	: International Organization for Standardization
JFIF	: JPEG File Interchange Format
JPE	: Associate with JPEG
JPEG	: Joint Photographic Experts Group
JPG	: Associate with JPEG
PassPix	: Passphrase Pixel
PDA	: Personal Digital Assistant
PIN	: Personal Identification Numbers
PNG	: Portable Network Graphics
PVAC	: Pixel Value Access Control
PX	: Pixel
RGB	: Red, Green, and Blue

CHAPTER 1

INTRODUCTION

1.1 Research Background

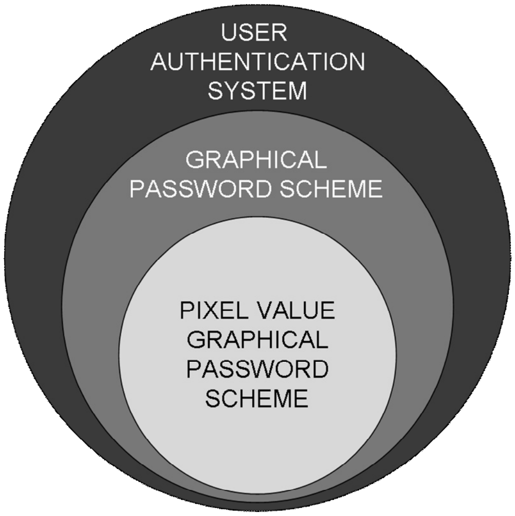

USER AUTHENTICATION SYSTEM
GRAPHICAL PASSWORD SCHEME
PIXEL VALUE GRAPHICAL PASSWORD SCHEME

Figure 1.1: Research area

Electronic authentication is the process of establishing confidence in user identities, electronically presented to an information system (Zissis et al., 2012). Authentication through username and alpha-numeric password is a way of computer authenticating its owner. On each subsequent use, the user must know and use the pre-declared password to guarantee that the user is authentic. However, in most of the cases, users very often choose bad passwords that are easy to guess, too short, or written down where others may discover it (Hyppönen, 2012). A longer pass-phrase with complex combination of alphabet, numeric and symbols is the safest text-based password structure but is hard to memorise. As an initiative to reduce this burden, the graphical password scheme was introduced where psychology studies have recognised the human brain's apparently superior memory for recognising and recalling visual information as opposed to verbal or textual information (Biddle et al., 2012). Click-based graphical password was the earliest technique of graphical password scheme that pioneering varieties of graphical password scheme have been designed and developed through various researches. Major focus of this research is another graphical password technique that used pixel value as an authentication approach to improvise click-based graphical password scheme.

1.2 Problem Statement

Click-based graphical password scheme requires user to click on several click-points or image sets which appear on login screen during the authentication process. The clickable password that appears to all users causes several issues (Biddle et al., 2012) which are:

a. Password guessing attempt since it is clickable by everyone
b. Too many click-objects on login screen causing login screen too crowded and more difficult to identify the click-object
c. However, using a small number of click objects, causing the password space to become smaller and easy to be guessed and increasing the success rate of try-and-error click attempt

1.3 Research Objectives

To work out and improvise on problems stated in Section 1.2, this research embarked on several objectives as below:

1. To investigate the features to solve and improvise the exposed and clickable graphical password features
2. To design a method based on the identified set of features to solve exposed and clickable graphical password features
3. To test and study the compliances of designed method

1.4 Research Scope

Graphical password was introduced to solve human memory burden on text-based password where a strong password was commonly hard to memorise. One of the methods introduced in graphical password scheme was click-based graphical password that requires user to click on an image click-points or image set causing security vulnerability issues as discussed in section 1.2. Literature study of this research will discuss vulnerabilities of exposed clickable image password. Literature review study and analysis conclude a set of features and characteristics of graphical password to solve the vulnerabilities of click-based graphical password scheme. The set of features and characteristics is a guideline to design and develop pixel value graphical password, a graphical password method to solve vulnerabilities on exposed and clickable password. Assuming that hosting system is well hardened, testing and finding analysis on the prototype of pixel value graphical password was fully based on client side or user side implementation.

1.5 Research Significance and Contribution

Click-based graphical password scheme has evolved on each new method proposed through a lot of researches and developments to solve vulnerabilities issues on previous method. However, most of the methods adapting the exposed and clickable image click-points or image set during user authentication stage. Through this research, a method that is proposed will solve vulnerability issues on clickable and exposed password on various method of current click-based graphical password scheme. The method itself will bring a lot of benefits to user while dealing with graphical password during authentication stage of a computer system such as:

a. Information of user's password is confidential and protected

b. User's password cannot be attempted by anyone

1.6 Thesis Organisation

This thesis contains seven chapters and is organised in sequence as follows:

1. Chapter 1 is the introduction chapter that introduces the idea of this research and elaborates on the background of this research
2. Chapter 2 is the literature review chapter that will elaborate on the current authentication system and graphical password scheme design and implementation
3. Chapter 3 is the research methodology that will elaborate on the method of finding, development, testing and analysis
4. Chapter 4 is where the pixel value graphical password scheme is briefly described in terms of concepts, design and workflow
5. Chapter 5 is implementation and testing where description testing on proposed method is described briefly
6. Chapter 6 is the result and discussion where all of the testing results and findings are discussed briefly in this chapter
7. Chapter 7 will conclude this thesis and discuss on extended discussion
8. References chapter contains the list of all references used in this research and thesis

1.7 Summary

Motivation of this research is to solve client side security vulnerability issues on exposed and clickable password on current various methods of click-based graphical password scheme. Solving the vulnerabilities will secure the user's graphical password while dealing with the graphical password scheme.

Next chapter will briefly discuss current authentication problems and exemplify several graphical password scheme methods that construct ideas to solve the problems.

CHAPTER 2

LITERATURE REVIEW AND ANALYSIS

2.1 Authentication System

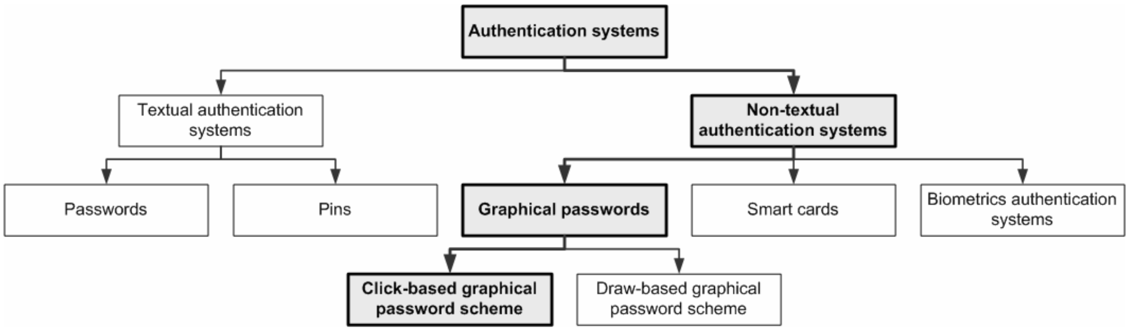

Authentication systems
Textual authentication systems
Non-textual authentication systems
Passwords
Pins
Graphical passwords
Smart cards
Biometrics authentication systems
Click-based graphical password scheme
Draw-based graphical password scheme

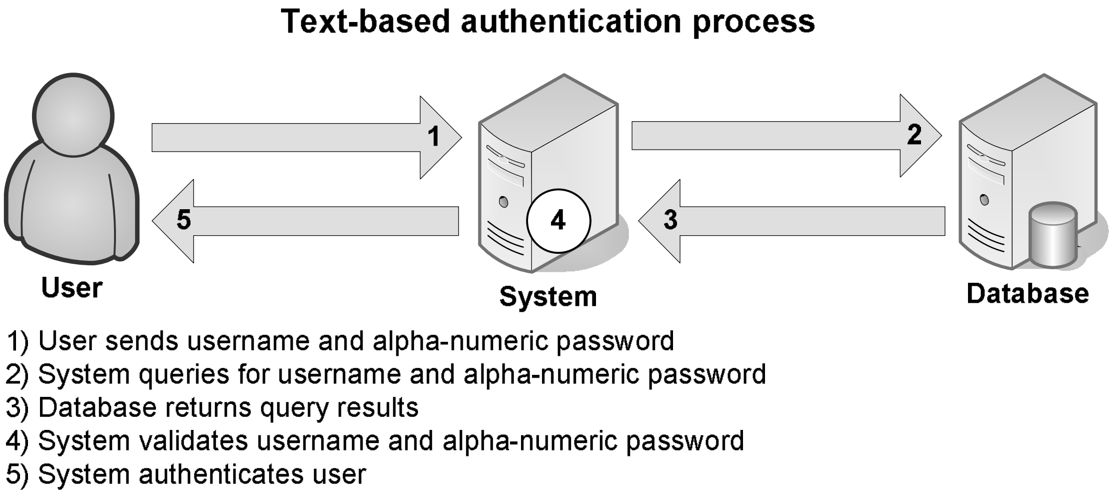
Figure 2.1: Division of authentication system

An authentication system comprises an authentication enforcement engine adapted to interface with an authentication provider for performing an authentication process for a user requesting access to a computer resource (Valiudin & Novoa, 2005). Authentication factors can be placed into three categories, namely what you know (password, secret, personal identification number); what you have (token and smart card) and what you are (biometrics and behavioural) (Mohammed et al., 2013). A blind credential, in contrast, does not establish identity at all, but only a narrow right or status of the user or program while as web trust, "authentication" is a way to ensure users are who they say they are—that the user who attempts to perform functions in a system is in fact the user who is authorised to do so (Hung, 2007). Passwords and PINs are susceptible to cracking attacks – an automated process of systematically trying all combinations until a match is found, pushed toward two differing authentication techniques: smartcards – the notion of ‘what you have’: and, biometric authentication – the notion of ‘what you are’. Most users are more familiar with smartcards than they realise; EFT cards that require PINs fit the profile of the smartcard architecture that is used in computing authentication but are more commonly implemented for access control and physical security (Pierce et al., 2004; Eljetlawi, 2008). Biometrics authentication that measures a physical or behavioural attribute of humans to uniquely identify them could relieve users from carrying smartcards and forgetting passwords as it measures physical parts and they cannot forget. Physical biometrics include fingerprint, iris, retina, face, voice, and deoxyribose nucleic acid (DNA) while behavioural biometrics include handwriting (graphology) and keystroke analysis. Biometric-based authentication requires specific input device or tools to enable computer to be read and translated into computer signal making it less popular to be implemented on the computer system by most developers and is less preferred by user. Of course the degree to which people’s privacy is invaded depends on the type of biometric used, the sensitivity of the information, and the possibility for combining data with other databases (Pierce et al., 2004; Eljetlawi, 2008).

2.2 Textual Password

Computer authentication has traditionally centered on ‘what you know’ which is embodied in textual-passwords that has exemplified in well known issue which is user finds it hard to memorise a strong password. In fact, it is a widely accepted fact that majority of users' passwords can be found written down within 4 feet of the workstation (Berger et al., 2003; Eljetlawi, 2008). In most of the time, users must authenticate separately to each system or application where users must repeatedly type their passwords and users are likely to choose less-than-secure passwords for convenience. Passwords that easily guessed are known as weak or vulnerable; very difficult or impossible to guess passwords are considered strong (Haque et al., 2012).

A strong password is which is sufficiently long and random will require too much resources while a weak password could be short and using common dictionary wordings which consumes less resources. The longer and the wider the variety of symbol choices, the more intensive the password cracking effort or well matched the Rainbow Table must be to defeat the password (Eljetlawi, 2008). The terms weak and strong are relative and quality of the password depends on how well the password system limits attempts to guess passwords. A study by Oorschot and Thorpe (2005) found that about 25% of 14,000 passwords were cracked by a dictionary with only 3 million entries (the size of the dictionary is 21.5 bits) by using a 3.2GHz Pentium 4 machine in only 0.22 second. Therefore, it is widely believed that the security of a password scheme is related more closely to the size of its memorable password space, rather than that of its full password space (Tao, 2006).



Text-based authentication process

1) User sends username and alpha-numeric password
2) System queries for username and alpha-numeric password
3) Database returns query results
4) System validates username and alpha-numeric password
5) System authenticates user

Figure 2.2: Textual-based authentication model

2.3 Graphical Password

Research in the psychology discipline has shown that images are more memorable than words or sentences (Gao et al., 2013). We can use this innate ability in humans for authentication in a similar way to recall passwords (Eljetlawi, 2008). Therefore, the graphical password scheme was introduced in middle of 90s to replace the textual password scheme and solve the issue of memorising a strong password. The idea behind graphical passwords is to leverage human memory with visual information, with the shared secret being related to or composed of images or sketches (Biddle et al., 2012). It requires user to click on the correct image in the correct sequences or draw the correct password texture based on grids or points during authentication stage. Knowledge-based (what you know) techniques are the most widely used authentication technique and include both textual and graphical passwords. The earliest design for graphical password scheme was initiated in 1996 that required users to touch