CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

This chapter defines background, problem statement, research questions, research objectives and thesis structure for this research. Other than that, this chapter presents the research scope that relates to the problem and significance of this research.

1.2 BACKGROUND

Password usually refers to a secret used for authentication. This is the most commonly used authentication and method for identifying users in computer systems. A graphical password is an authentication system that works by having the user to select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA). There is an alternative to alphanumeric passwords in which users click on images to authenticate themselves rather than type alphanumeric strings. Authentication is the principal method to guarantee information security and the most common and convenient method is password authentication (Renaud, 2005).

Traditional alphanumeric passwords are strings of letters and digits, which are easy and familiar to essentially all users. However, there are several inherent defects and deficiencies in alphanumeric passwords, which easily evolve into security issues. Due to the limitation of human memory, most users tend to choose short or simple passwords, which are easy to remember (Adams & Sasse, 1999). Surveys show that

frequent passwords are personal names of family members, birth date, or words available in dictionaries. In most cases, these passwords are easy to guess and vulnerable to dictionary attack (Pilar et al., 2012).

Today, users have many passwords for personal computers, social networks and E-mail. They may decide to use one password for all systems to decrease the memory burden, which reduces security (Stobert & Biddle, 2013). Like alphanumeric passwords, graphical passwords are knowledge-based authentication mechanisms. The main goal of graphical passwords is to use images or shapes to replace text, since numerous cognitive and psychological studies demonstrated that people perform far better when remembering images than words, because human factors are often considered the weakest link in a computer security system (Ambekar & Welekar, 2015). The most widely accepted theory explaining this difference is the dual-coding theory (Paivio, 2006), suggesting that verbal and non-verbal memories are processed and represented differently in the mind. Assigned with perceived meaning based on direct observation, the images are represented in a way that retains the perceptual features being observed. The text is represented with symbols that convey associatively cognitive meaning.

As the result, additional processing required for verbal memory renders a more difficult cognitive task. Thus it is easy for human being to remember graphic images such as faces of people, places they visit, type of foods and things they have seen for a lengthy duration (Seng et al., 2011). Based on the previous studies and research, many graphical authentication schemes have been deployed today, for examples, Windows 8 picture password and Android lock screen (Stobert & Biddle, 2013).

1.3 PROBLEM STATEMENTS

The vulnerabilities of the textual password have been well known. Users tend to pick short passwords or passwords that are easy to remember, which makes the passwords vulnerable for attackers to break. Furthermore, textual password is vulnerable to guessing, dictionary attack, key-loggers, social engineering, shoulder surfing, and spyware attack (Saranya and Bindhu, 2014). Techniques of two-factor authentication and graphical password have been put in use to conquer the limitations of text-based password. As the technology become advance day by day, the crackers also tend to be more creative to manipulate the graphical password or to steal the information. They also use the same technique to attack the graphical password, such as shoulder surfing and brute force attack (Saranya and Bindhu, 2014).

Nowadays, researchers are enhancing the authentication systems based on the graphical authentications. However, there are several deficiencies with the graphical password authentication using the existing method based on the usability and security perspectives. Based on the implication, current researches and opportunities, there is a need to develop a new graphical password authentication to overcome their limitations in terms of usability and security. In Addition, no studies have been reported previously, specifically on combination of three graphical authentications: choice-based, click-based, and draw-based. It is because the combination of graphical authentication schemes promise to provide better security (e.g. larger password space). Therefore, to fill the gap of current deficiency of graphical password authentication, this thesis proposed a new development of authentication scheme that is based on the hybrid schemes.

1.4 RESEARCH QUESTIONS

Based on the problem statements above, the number of questions arose that need to be addressed such like:

a) What is the current development state and challenges in graphical authentication schemes?

b) How to enhance the features of graphical authentication that uphold security, while maintaining usability?

c) Can hybrid graphical authentication make a good alternative to the existing password authentication?

1.5 RESEARCH OBJECTIVES

This work tries to fulfil the following objectives based on the abovementioned research questions:

i. To further study the current graphical password authentication in the relation of usability and security.

ii. To design and develop new graphical authentication scheme prototype.

iii. To conduct evaluation on the developed prototype.

1.6 RESEARCH SCOPE

The main aim in the thesis is to develop alternative graphical authentication scheme. Evaluations towards new graphical authentication were conducted with regards to its usability and security. In addition, the evaluations were made with the specific objectives of identifying several factors like users' familiarity, timing and pattern of graphical passwords. Majority of the participants were obtained through an open call

for volunteer, who were mainly consisted of students of different backgrounds. Table 1.1 summarises the research scope applied throughout all studies within the thesis; starting from the literature review until the development and tests conducted.

Table 1.1: Relation of research questions, research objectives and justifications

No	Research Questions	Research Objectives	Research Activities / Tasks
1	What is the current development state and challenges in graphical authentication schemes?	To further study the current graphical password authentication in the relation of usability and security.	Reviewing literatures regarding graphical authentication and making comparative studies.
2	How to enhance the features of graphical authentication that uphold security, while maintaining usability?	To design and develop new graphical authentication scheme prototype.	Developing a prototype of graphical scheme with hybrid graphical scheme (combination of three graphical authentication).
3	Can hybrid graphical authentication make a good alternative to the existing password authentication?	To conduct evaluation on the developed prototype.	Conducting empirical studies and analyse all of the data after the evaluation have done.

1.7 THESIS STRUCTURE

The rest of this thesis is organized as follows. Chapter 2 highlights the literature review related to existing of graphical authentication in aspect of usability and

security. Then, Chapter 3 introduces the methodology used for the research tools and environment as whole. Next, Chapter 4 explained about the development of new graphical password prototype based on hybrid scheme called ChoCD and discusses the design of the authentication to fulfil the usability requirements. Chapter 5 discusses the studies conducted to investigate the practicability of ChoCD. Evaluations towards ChoCD authentication were conducted with regards to its usability and security. It involves the explanation of its methodology, results and findings, and discussion. Chapter 6 summarises the overall thesis by presenting achievements with respect to the conduct of this research. In addition, this chapter also highlights the limitations identified while the research had been conducted, and finally presents potential future works for improving the limitation of the present research.