CHAPTER I

INTRODUCTION

1.1 BACKGROUND

The first chapter of the research determines the problem statement, research questions, research objectives, research scope and limitations. Furthermore, this chapter states the concepts that relate to the problem, significance, research output and the existing researches that associated with the research topic.

Nowadays, there are a lot of ways to attack and steal the personal information such as passwords. One of these ways is the social engineering technique as; attention-grabbing subject, trusted e-mail source, confidence-building, reverse social engineering (RSE), piggybacking tactic, techie talk tactic, a phishing attack, a spear phishing attack, social networking sites attacks and guessing attack. So, it is becoming necessary to find techniques that protect the information from the attacks, one of these ways is the using of the graphical password that has a various types with a different features for each of them.

The idea of graphical password (GP) means the passwords that based on images rather than traditional password (TP) (Por *et al.,* 2008). Graphical passwords are categorized

into three types: Click based graphical password scheme, choice based graphical password scheme and draw based graphical password scheme (Biddle *et al.*, 2009; Por *et al.*, 2008). Click-based graphical password scheme consists of various click points on a single image or photo, while in the choice-based graphical password the user click on different images. However, in draw-based graphical password the secret password is drawn on the selected image (Shrikala *et al*., 2013; Chitrey, 2012).

Social engineering is a process that tries to obtain confidential information. It is a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. Social engineers rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it (Shrikala *et al.*, 2013; Guenther, 2001).

Social engineering attacks could be defined as the process to penetrate the systems and obtain information illegally and using non-technical methods, but through the exploitation of human weaknesses (Social engineering based on using a series of tricks to gain the information such as user name and password, also it is possible to exploit the information contained in the trash (Sun *et al.*, 2012).

The social engineering technician could claim that is working with the technical team at the company and wants to get the password to solve the computer system problems and the database for the company. Whenever people use services such as e-bank and e-mail, servers ought to have the skills to authenticate the users' identities. Otherwise, any person can easily impersonate a legal user to login to the server (Chitrey *et al.*, 2012).

Password-based authentication schemes are simple and practical solutions to the user identified because they permit people to select their own passwords without any mechanism to generate or store them. For personal computers, passwords contain letters, numbers, and unique punctuations on a standard QWERTY keyboard. This is called alphanumeric-based password authentication (Por *et al.*, 2008; Sun *et al.*, 2012).

Users typically handle with text-based password problems as follows: First, they note down their passwords; second, they employ one password for several systems; third, natural language phrases are preferably used as passwords so they can be recognized easily. However, this leads to some text-based passwords becoming weak passwords that are vulnerable to dictionary and shoulder surfing attacks (Sun *et al.*, 2012; Biddle *et al.*, 2009).

Recently, touch screen handles mobile devices have been becoming more widespread. A user inputs his or her password by clicking or touching the touch panel, so a recognition-based graphical password authentication system for mobile devices is proposed. Jansen's system divides an image into thirty thumbnail photos (Shrikala e*t al*., 2013; Biddle *et al*., 2009; Jansen, 2004).

A user selects numerous different thumbnail photos and the sequence of these thumbnail photos is the user's graphical password. Therefore, the password space size is larger than before. For example, a user chooses three photos and then the password space size is enlarged from 30 × 29 × 28 to 303. However, Jansen's methods still

cannot withstand shoulder surfing attacks (Shrikala e*t al*., 2013; sun *et al*., 2012; Biddle *et al*., 2009; Jansen, 2004).

1.2 PROBLEM STATEMENT

Many researchers have studied the traditional passwords attacks. The researchers agreed that the traditional passwords are easy to penetrate by all kinds of attacks methods such as; brute force, dictionary, guessing, spyware and loggers, shoulder surfing and social engineering attacks (Dunphy, 2013; Lashkari *et al*., 2012 and Khan *et al*. 2011).

The graphical passwords (GP) attacks were studied (Dunphy, 2013; Stobert *et al*., 2010; Khan *et al*. 2011; Almaula, 2008), such as; brute force, dictionary, guessing, spyware and loggers, shoulder surfing and social engineering attacks. But a few researchers examine the effect of social engineering attack techniques on graphical passwords types; since there are a huge amount of techniques in social engineering attacks, and it develops rapidly based on the development of the technology.

Based on the aforementioned statement, this thesis examines **the effects of social engineering attack techniques on the graphical passwords types (GP). Moreover, the study identifies the best graphical password type that has the ability to resist the social engineering attack techniques**.

1.3 RESEARCH QUESTIONS

The study seeks to answer the following questions;

1- Is the method of social engineering attacks in traditional passwords similar to the graphical passwords?

2- Which graphical password method is the best and can resist social engineering attacks?

1.4 RESEARCH OBJECTIVES

This research aims to achieve the following objectives:

1- To study the social engineering techniques;

2- To study the effect of social engineering techniques on traditional and graphical password authentications.

3- To evaluate the best type of graphical password that is secure.

1.5 RESEARCH SCOPE AND LIMITATIONS

This study is interested in information security through emphasis the social engineering techniques and its impact on the authentication techniques such as traditional passwords and graphical passwords. It also tries to select the best graphical passwords that resist the social engineering attacks.

This study utilizes the guessing attacks as a branch of social engineering techniques to obtain the needed password by the participants. It is one of the most important ways

of the social engineering techniques. It is based on the ability of the attackers to guess the victims' password. This method is based on exploiting the confidence of the victim to get the personal information and then to guess the password.

The role of the participants in this study is to guess the choice-based graphical password and click-based graphical password; since the choice-based graphical password and the click-based graphical password depend on choosing from a specific photo unlike draw-based which creates a new drawing by the users. At this study no relationship analysis attempt were made, just enough with the descriptive statistics using SPSS, as the study seek to identify the correct passwords that the participants managed to guess.

1.6 RESEARCH CONTRIBUTIONS

This research has been published in "International Conference on Advances in Computing, Electronics and Electrical Technology, CEET- 2014". The copy of acceptance letter and review result is attached in appendixes (Appendix B and Appendix C). The actual paper is as in the Appendix D.

1.7 THESIS ORGANIZATION

The thesis consists of five main chapters, each chapter covers a specific part of the research as the following arrange: Chapter I is introduction, it introduces the thesis, determines the problem statement, research questions, research objectives, research scope and limitations. Chapter II is literature review; it illustrates various opinions and

views in social engineering and graphical passwords from the existing researches. Chapter III explains research methodology, while Chapter IV presents results from data collection and analysis. Finally, Chapter V concludes the thesis by presenting our though on the conduct of the study and potential future works.