CHAPTER V

CONCLUSION

5.1 INTRODUCTION

This chapter highlights the achievement of the objectives, and also presents the contribution to the knowledge. The chapter ends with the list of future works that potentially been done.

5.2 ACHIEVEMENT

This study demonstrated that there are many means for social engineering. For example social engineering attacks can be defined as the way that is widely used by the attackers because it is the easiest way to gain the access to confidential information or carry out other security-related attacks on information systems (Mitnick & Simon, 2002; Karpati *et al*. 2012).

UNIVERSITI SAINS ISLAM MALAYSIA
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

of all of these, the study grouped social engineering techniques (SET) into four main classifications; confidence, greed, curiosity and human psychology.

The first group consists of the techniques that based on exploiting the victim's confidence by the attackers then they can obtain the wanted information. These techniques are; trusted domain, vishing (voice phising attacks), piggy-backing tactic, confidence building, trusted e-mail sources, whaling attack, generic sender, attention-grapping subject, guessing attack, reverse social engineering attack (RSE) and techie-talk tactic.

The second group consists of techniques based on greed; the attackers exploiting the victim's greed to obtain the needed information, for example by presenting a financial prize. These techniques are spear phishing and phishing attacks.

The third group is based on the curiosity; where the attackers exploiting the victims' curiosity such as knowing a new person to obtain the desired information. These techniques include the social networking sites attack and exploiting the sex attack.

Finally, the fourth group consists the techniques that the attackers exploiting the human psychology to obtain the information. These techniques depend on the ability of the attackers to read the physical language of the people, read the reflexes and the ability to observe behavioral patterns of people, practices, and then exploit all these aspects to gain the trust of the people to get the information. Neuro-linguistic programming (NLP) attacks and exploiting humans' problems are an examples of this group.

UNIVERSITI SAINS ISLAM MALAYSIA
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

A study of social engineering techniques has been conducted towards both traditional and graphical passwords, and found that not all techniques were vulnerable. This is due to the fact that of nature of the method themselves. The result of comparing social engineering techniques with both traditional password (TP) and graphical password (GP) is as in the Table 17.

TABLE 17: SET Towards Graphical and Traditional password.

Social Engineering Attack Techniques	**GP**	**TP**
1-Attention-grabbing subject	×	√
2-Trusted e-mail source	√	√
3-Confidence-building	×	√
4-Trusted domain	×	√
5- Generic sender	×	√
6-Reverse social engineering	×	√
7- Piggybacking Tactic:	×	√
8- Techie Talk Tactic:	×	√
9- A phishing attack:	√	√
10- A Spear Phishing Attack:	√	√
11- A Whaling Attack:	×	√
12- Vishing (voice phishing) attack:	×	√
13- Social networking sites Attacks:	×	√
14-Neuro-linguistic programming (NLP) Attacks	×	√
15- Exploiting the Sex:	×	√
16- Exploiting humans' problems	×	√
17-Guessing attacks	√	√
√= yes ×= No		

The research then proceeds to investigate the best graphical password that prone to social engineering techniques. The study decided to investigate a guessing attack, a branch of social engineering techniques.

Generally, participants participated needed to guess a series of images (in the case of choice-based) and a series of clicks (for the click-based) from the set of given images and clicks.

From the analysis of results, it was found that the participants who guessed the click-based password are more than the participants who guessed the choice-based password. Therefore, this research concludes that the authentication based upon choice was resistant and superior as compared to the authentication based upon click.

5.3 CONTRIBUTION

The contributions of this research are as the following:

1- This research managed to classify social engineering techniques into four classifications, as discussed earlier.
2- Extensive comparative of social engineering techniques towards traditional password and graphical password was presented.
3- Conducted a study to compare click-based and choice-based graphical passwords towards one social engineering attacks known as guessing attack.

5.4 POTENTIAL FUTURE WORKS

This study can be improved by examination the effect of social engineering attacks on the three types of graphical password (choice-based, click-based and draw based) to determine the best type that could be used. Another way is by studying the impact of several techniques (social engineering attacks and brute attacks) on the graphical password types.

5.5 SUMMARY

This research achieves its main objectives which they are; study the social engineering techniques on both traditional and graphical password, in addition to examine the impact of social engineering techniques on choice-based and click-based graphical password.

Social engineering involves several methods and techniques to access the information and penetrate accounts (Guenther & Broadhurst, 2006); attention-grabbing subject, trusted e-mail source, confidence-building, trusted domain, generic sender, reverse social engineering, piggybacking tactic, techie talk tactic, a phishing attack, a spear phishing attack, a whaling attack, vishing (voice phishing) attack, social networking site's attacks, neuro-linguistic programming (NLP) attacks, exploiting the sex, exploiting humans' problems and guessing attack. They were classified into four groups depending on the exploitation of one of the weaknesses.

Fifty participants of university students fill in the questionnaires. The results show that the authentication based upon choice was resist and superior as compare to the authentication based upon click.

These results are satisfied; the choice-based graphical password is more difficult to guess in comparing with the click-based graphical password since there is a vast amount of photos. While, the probability to guess the password in click-based is more since there is a specific photo.

UNIVERSITI SAINS ISLAM MALAYSIA
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية الماليزية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA