

## AUTHOR DECLARATION

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

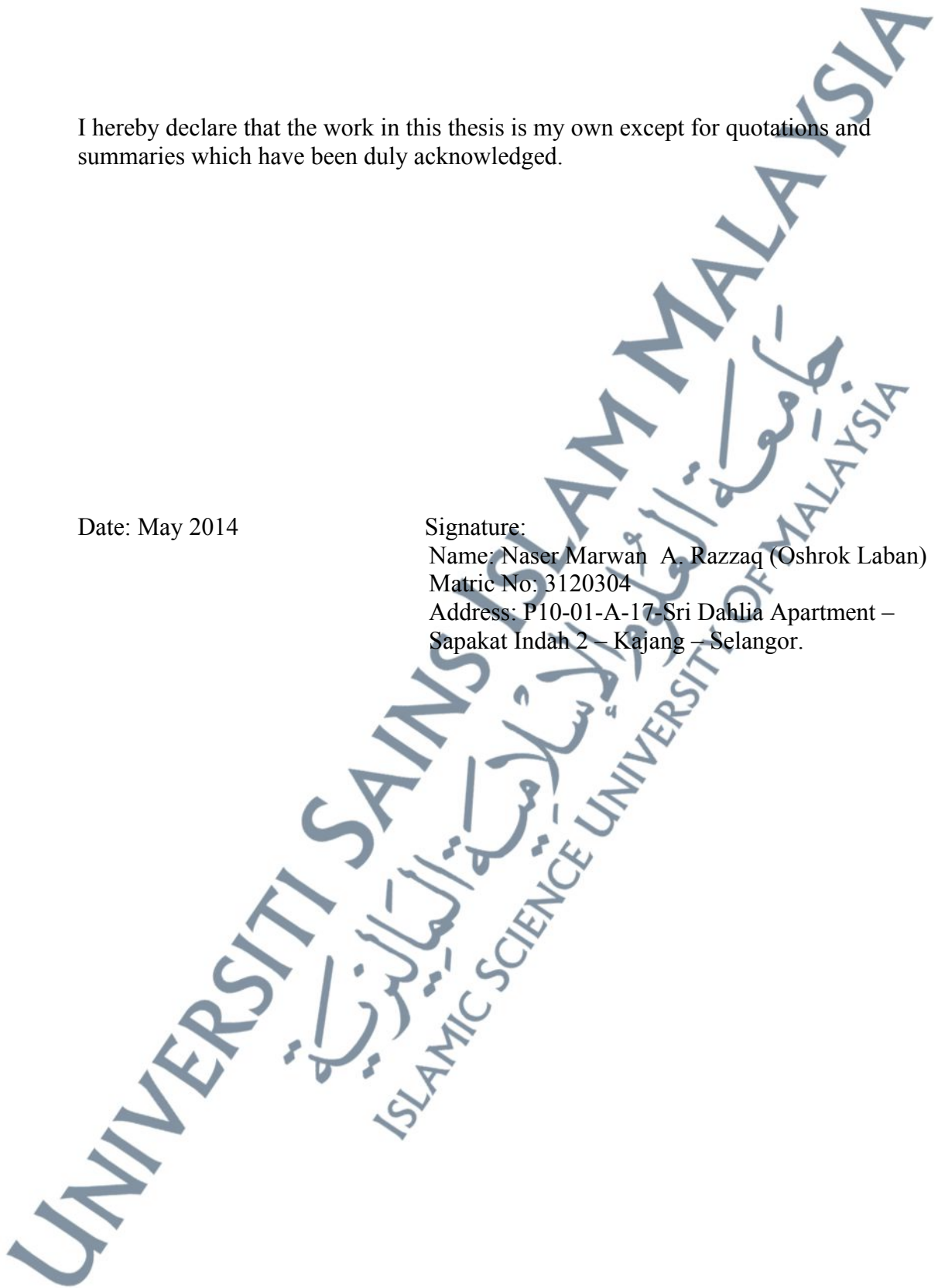
Date: May 2014

Signature:

Name: Naser Marwan A. Razzaq (Oshrok Laban)

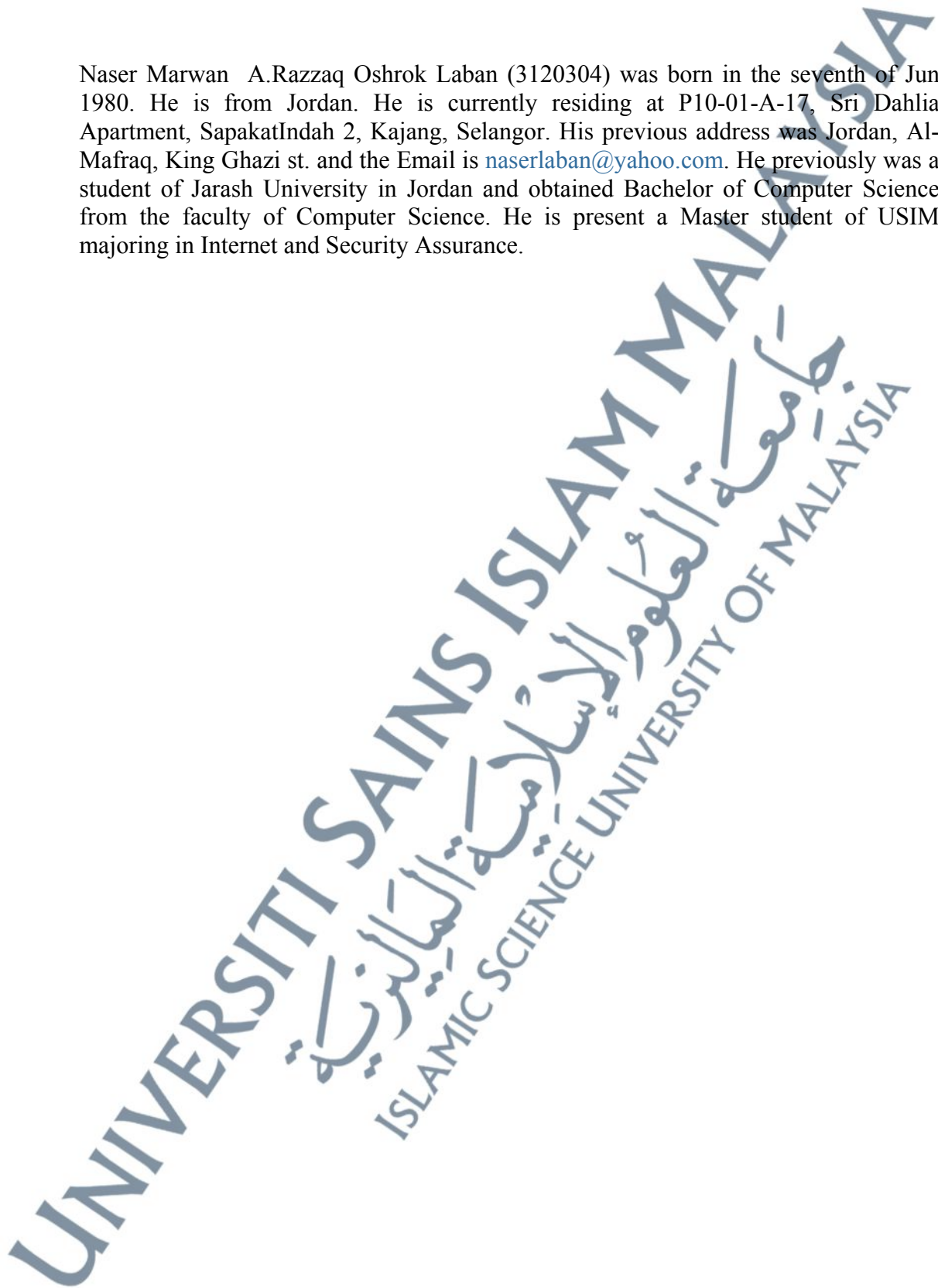
Matric No: 3120304

Address: P10-01-A-17-Sri Dahlia Apartment –  
Sapakat Indah 2 – Kajang – Selangor.



## BIODATA OF AUTHOR

Naser Marwan A.Razzaq Oshrok Laban (3120304) was born in the seventh of Jun 1980. He is from Jordan. He is currently residing at P10-01-A-17, Sri Dahlia Apartment, SapakatIndah 2, Kajang, Selangor. His previous address was Jordan, Al-Mafraq, King Ghazi st. and the Email is [naserlaban@yahoo.com](mailto:naserlaban@yahoo.com). He previously was a student of Jarash University in Jordan and obtained Bachelor of Computer Science from the faculty of Computer Science. He is present a Master student of USIM majoring in Internet and Security Assurance.



## ACKNOWLEDEMENTS

Grateful to Allah SWT and his Messenger Muhammad SAW for the Islam. Appreciation and acknowledge the important contributions and guidance provided by Dr. **Mohd Zalisham Jali** to completion this thesis.

Great thanks are due to the deans of faculties and heads of departments of USIM for cooperation in the survey questionnaire, and without their generous support data would lack in accurate information on current thesis.

In addition, thanks are due to all my friends taking part in the study. Great thanks also to my mother, my wife and my children.

Naser Marwan A. Razzaq (Oshrok Laban)

## ABSTRAK

Sejak kebelakangan ini, kejuruteraan sosial telah diberi penekanan dan pertimbangan sebagai salah satu proses untuk menembusi benteng keselamatan maklumat dan informasi samada terhad atau tidak. Teknik kejuruteraan sosial yang dimaksudkan adalah satu halacara atau kaedah memperoleh maklumat atau informasi tanpa kebenaran pemiliknya atau tanpa kebenaran formal pemiliknya bagi menembusi akaun-akaun melalui penggunaan halacara atau metod-metod yang bukan teknikal secara godaman yang bergantung kepada kemahiran penggadam dengan menggunakan kebijaksanaannya untuk menipu orang lain dan memaksa mereka memperoleh sebanyak bolih maklumat dan informasi yang dikehendaki. Masa kini, teknik-teknik kejuruteraan social ini disalahguna sebagai halacara atau kaedah yang paling kerap digunakan untuk memerangi serta mencuri maklumat dan informasi di seluruh dunia kerana ianya telah menjadi satu keperluan bagi mengkaji berbagai cara mencerooboh dan menentukan kaedah-kaedah yang melindungi maklumat dan informasi dari digodam atau diperangi seperti dengan menggunakan katalaluan ("*password*") grafik. Katalaluan grafik ini adalah satu sistem otentikasi (*authentication*) yang bolih digunakan oleh mana-mana pengguna dengan memilih imej-imej mengikut aturan tertentu yang disediakan dalam bentuk bersemuka (*interface*) pengguna grafik (*Graphical User Interface, GUI*). Oleh yang demikian, kaedah katalaluan grafik ini kadangkala dikenali sebagai otentikasi pengguna secara grafik (*Graphical User Authentication, GUA*). Terdapat tiga jenis katalaluan grafik yang kerap digunakan; berasaskan pilihan katalaluan grafik, berasaskan klik (*click*) katalaluan grafik dan berasaskan lukisan katalaluan grafik. Disamping itu katalaluan tradisi ialah perkataan rahsia atau karakter-karakter yang digunakan untuk otentikasi pengguna dan identitinya bagi mendapat akses kepada sumber-sumber maklumat dan informasi berkenaan. Tujuan utama kajian ini adalah untuk menjelaskan dengan terperinci kaedah-kaedah penggodaman kejuruteraan sosial ke atas kedua-dua kaedah katalaluan grafik dan katalaluan tradisi dengan membuat rujukan kepada hasil-hasil kajian terdahulu serta bahan-bahan bacaan berkaitan yang terkini. Dalam pada itu, tesis ini juga akan merangkumi kajian yang dijalankan dengan berjumpa dengan responden secara rawak bagi membanding katalaluan grafik berasaskan klik dan berasaskan katalaluan pilihan terhadap mencipta dan merekabentuk katalaluan, iaitu satu cabang kaedah kejuruteraan sosial. Bagi mencapai matlamat objektif ini satu kajian dilapangan dijalankan dengan menggunakan kaedah pengisian borang soalan kepada sekurang-kurang 50 responden atau peserta kajian. Data dan fakta-fakta yang dikumpulkan dianalisa menggunakan teknik SPSS. Hasil kajian yang dijalankan menunjukkan bahawa katalaluan grafik berasaskan pilihan bolih bertahan dengan baik terhadap godaman lebih daripada katalaluan grafik berasaskan klik.

## ABSTRACT

Social engineering has been considered as one of the main processes to break through the information security. Social engineering technique is the way to get unauthorized information and penetrating accounts through the use of non-technical methods relying on the skills of the hacker in the ability to deceive others and persuade them to get as much information. Social engineering techniques are considered the most ways that are used to attack and steal the information all over the world, for that it is becoming necessary to study this kind of attacks and find methods that protect the information from the attacks such as graphical password. A graphical password is an authentication system that works by having the user 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 are three graphical password types; choice-based graphical password, click-based graphical password and draw-based graphical password. On the other hand traditional password is a secret word or characters used for the user's authentication and identity to gain access to resources. The aims of this study are to thoroughly explain social engineering attacks methods, classified the social engineering attack methods based on the weaknesses and compare the impact of the social engineering attacks methods on both of the graphical password and traditional password by referring to the existing literature reviews. In addition, the thesis will also present a study conducted to compare the graphical password types (click-based and choice-based graphical password) towards passwords guessing, a branch of social engineering methods. To achieve the research goals an extensive literature search was conducted to achieve the first and second objectives. For the third objective a survey was conducted by distributing a questionnaire to 50 participants. The data that collected by using the questionnaire were analyzed via SPSS. Results show that traditional passwords are easy to attack by all kinds of attacks, while, the graphical passwords are difficult to penetrate in comparative to traditional passwords. Moreover, choice-based graphical passwords can resist the attacks better than click-based graphical passwords as 3 persons guessed the click-based graphical password while 2 persons guessed the choice-based graphical password.

## ملخص البحث

في الآونة الأخيرة أعتبرت الهندسة الاجتماعية واحدة من العمليات الرئيسية التي تستخدم لاختراق أمن المعلومات. من الامثلة على ذلك تقنية الهندسة الاجتماعية حيث تعتبر السبيل للحصول على معلومات غير مصرح بها واختراق الحسابات من خلال استخدام وسائل غير تقنية بحيث انها تعتمد على المهارات الشخصية من قبل القراصنة بحيث تتطلب القدرة على خداع الآخرين وإقناعهم للحصول على أكبر قدر من المعلومات. في الوقت الحاضر، تعتبر تقنيات الهندسة الاجتماعية من أكثر الطرق التي يتم استخدامها لمهاجمة و سرقة المعلومات في جميع أنحاء العالم ، لذلك أصبح من الضروري دراسة هذا النوع من الهجمات وإيجاد الأساليب التي تحمي المعلومات من الهجمات مثل استخدام كلمة المرور الرسومية . كلمة المرور الرسومية هي عبارة عن نظام مصادقة يعمل من خلال اختبار عدد محدد من الصور بترتيب معين من ضمن مجموعة صور موجوده في واجهة التطبيق الرسومية للمستخدم. هناك ثلاثة أنواع لكلمة المرور الرسومية وهي: كلمة المرور الرسومية القائم على الاختيار وكلمة المرور الرسومية القائم على الضغط على جزء من الصورة وكلمة المرور الرسومية القائم على الرسم. من ناحية أخرى فإن كلمة السر التقليدية (النصية) هي كلمة أو مجموعة من الأحرف المستخدمة لمصادقة المستخدم و السماح له بالوصول إلى المعلومات الخاصة بحسابه. الأهداف الرئيسية لهذه الدراسة هي شرح أساليب هجمات الهندسة الاجتماعية، وتصنيف أساليب هجمات الهندسة الاجتماعية بناء على نقاط الضعف. و دراسة تأثير أساليب هجمات الهندسة الاجتماعية على كل من كلمة المرور التقليديه وكلمة المرور الرسومية و من ثم المقارنة بينها وذلك بالاعتماد على الدراسات السابقة للهندسة الاجتماعية وتأثيرها على كلمات المرور التقليديه والرسومية. بالإضافة إلى ذلك، فإن هذا البحث يقدم أيضا دراسة أجريت للمقارنة بين أنواع كلمة المرور الرسومية ( كلمة المرور الرسومية القائم على الاختيار وكلمة المرور الرسومية القائم على الضغط) من حيث تأثيرهما بهجوم التخمين، وهو واحد من اساليب الهندسة الاجتماعية. لتحقيق هذا الهدف تم إجراء مسح عن طريق توزيع استبيان على 50 مشاركا . وقد تم تحليل البيانات الناتجة عن الاستبيان عن طريق برنامج التحليل الاحصائي، واطهرت النتائج بأن كلمة المرور الرسومية القائم على الاختيار لديها قدرة لمقاومة هجمات الهندسة الاجتماعية بشكل افضل من كلمة المرور الرسومية القائم على الضغط.

## TABLE OF CONTENTS

<b>CONTENTS</b>		<b>Page</b>
Title Page		i
Author Declaration		ii
Biodata of Author		iii
Acknowledgements		iv
Abstrak		v
Abstract		vi
Mulakhas Al-Bahth		vii
Tables of Contents		ix
List of Tables		x
List of Figures		xi
List of Appendices		xii
Abbreviations		
<b>CHAPTER I</b>	<b>INTRODUCTION</b>	<b>1</b>
1.1	Background	1
1.2	Problem Statement	4
1.3	Research Questions	5
1.4	Research Objectives	5
1.5	Research Scope and Limitations	5
1.6	Research Contributions	6
1.7	Thesis Organization	6
<b>CHAPTER II</b>	<b>LITERATURE REVIEW</b>	<b>8</b>
2.1	Introduction	8
2.2	Social Engineering Attacks	9
2.2.1	Social Engineering Attacks Definitions	9
2.2.2	Social Engineering Attacks Techniques	10
2.2.3	Social Engineering Attacks Classifications	14
2.2.4	The Social Engineering Attacks Cycle	18
2.2.5	Human Behaviors	21
2.3	Traditional Password and Graphical Password	24
2.3.1	Traditional Password	24
2.3.2	Graphical Password	25
2.4	Social Engineering Attacks Against Traditional Password and Graphical Password	28
2.5	Summary	33
<b>CHAPTER III</b>	<b>RESEARCH METHODOLOGY</b>	<b>35</b>
3.1	Introduction	35
3.2	Procedure of The Study	36
3.3	Data Collection	37
3.3.1	Participants	37
3.3.2	Structure of The Questionnaire	38
3.3.3	Steps Each Participants To Do	40
3.3.4	Data Analysis	42

3.4	Summary	42
<b>CHAPTER IV</b>	<b>RESULTS AND DISCUSSION</b>	<b>43</b>
4.1	Introduction	43
4.2	Results Related To Objective One	44
4.3	Results Related To Objective Two	46
4.4	Results Related To Objective Three	48
4.4.1	Demographic Data	48
4.4.2	Choice-Based Graphical Password	50
	Choice-based Graphical Password-First Attempt	50
	Choice-based Graphical Password-Second Attempt	51
	Choice-based Graphical Password-Third Attempt	52
	Compare Patterns' Repetition	53
4.4.3	Click-Based Graphical Password	55
	Click-based Graphical Password-First Attempt	55
	Click-based Graphical Password-Second Attempt	56
	Click-based Graphical Password-Third Attempt	57
	Compare Patterns' Repetition	58
4.4.4	The Questionnaire Result	60
4.6	Summary	61
<b>CHAPTER V</b>	<b>CONCLUSION</b>	<b>63</b>
5.1	Introduction	63
5.2	Achievement	63
5.3	Contribution	66
5.4	Potential Future Works	66
5.5	Summary	67
	Bibliography	68
	Appendices	73



## LIST OF TABLES

		Page
Table 1:	Common social engineering management attacks	15
Table 2:	Common social engineering mobile device attacks	15
Table 3:	Common social engineering personal attacks	16
Table 4:	Common social engineering reverse engineer attacks	16
Table 5:	Possible attack methods on graphical passwords	28
Table 6:	Traditional and graphical password attacks	46
Table 7:	Graphical and traditional password attacks references	47
Table 8:	Attempt one (Choice based graphical passwords)	50
Table 9:	Attempt two (Choice-based graphical passwords)	51
Table 10:	Attempt three (Choice-based graphical passwords)	52
Table 11:	Patterns repetition at the choice-based attempts	53
Table 12:	Attempt one (Click-based graphical passwords)	56
Table 13:	Attempt two (Click-based graphical passwords)	57
Table 14:	Attempt three (Click-based graphical passwords)	57
Table 15:	Pattern's repetition at the click-based attempts	58
Table 16:	The total correct passwords	61
Table 17:	Social engineering techniques towards graphical and traditional password	65

## LIST OF FIGURES

		Page
Figure 1:	Social engineering attack cycle	20
Figure 2:	Methodology phases	37
Figure 3:	Choice-based graphical password method	40
Figure 4:	Click-based graphical password method	40
Figure 5:	Social engineering methods classification	45
Figure 6:	Participant's gender	48
Figure 7:	Participant's universities	49
Figure 8:	Student's level of study	49
Figure 9:	Patterns repetition in the first attempt (choice-based)	51
Figure 10:	Patterns repetition in the second attempt (choice-based)	52
Figure 11:	Patterns repetition in the third attempt (choice-based)	53
Figure 12:	Compare the patterns' repetition of choice-based attempts	54
Figure 13:	Patterns repetition at the choice-based	55
Figure 14:	Patterns repetition in the first attempt (click-based)	56
Figure 15:	Patterns repetition in the second attempt (click-based)	57
Figure 16:	Patterns repetition in the second attempt (click-based)	58
Figure 17:	The patterns' repetition at click based	59
Figure 18:	Pattern's repetition at the click-based	60

**LIST OF APPENDICES**

	Page
Appendix A: The questionnaire	73
Appendix B: The acceptance letter	76
Appendix C: The Review result	78
Appendix D: Paper	79
Appendix E: Turnitin	84

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

## ABBREVIATIONS

CCP	Cued Click Points
GP	Graphical Password
GUA	Graphical User Authentication
GUI	Graphical User Interface
NLP	Neuro-Linguistic Programming
PCCP	Persuasive Cued Click Points
RSE	Reverse Social Engineering
SE	Social Engineering
SEA	Social Engineering Attacks
SEM	Social Engineering Methods
SET	Social Engineering Techniques
TP	Traditional Password