

**ChoCD: USABLE AND SECURE GRAPHICAL PASSWORD
AUTHENTICATION SCHEME**

Radhi Rafiee Bin Afandi
(Matric No: 3150100)

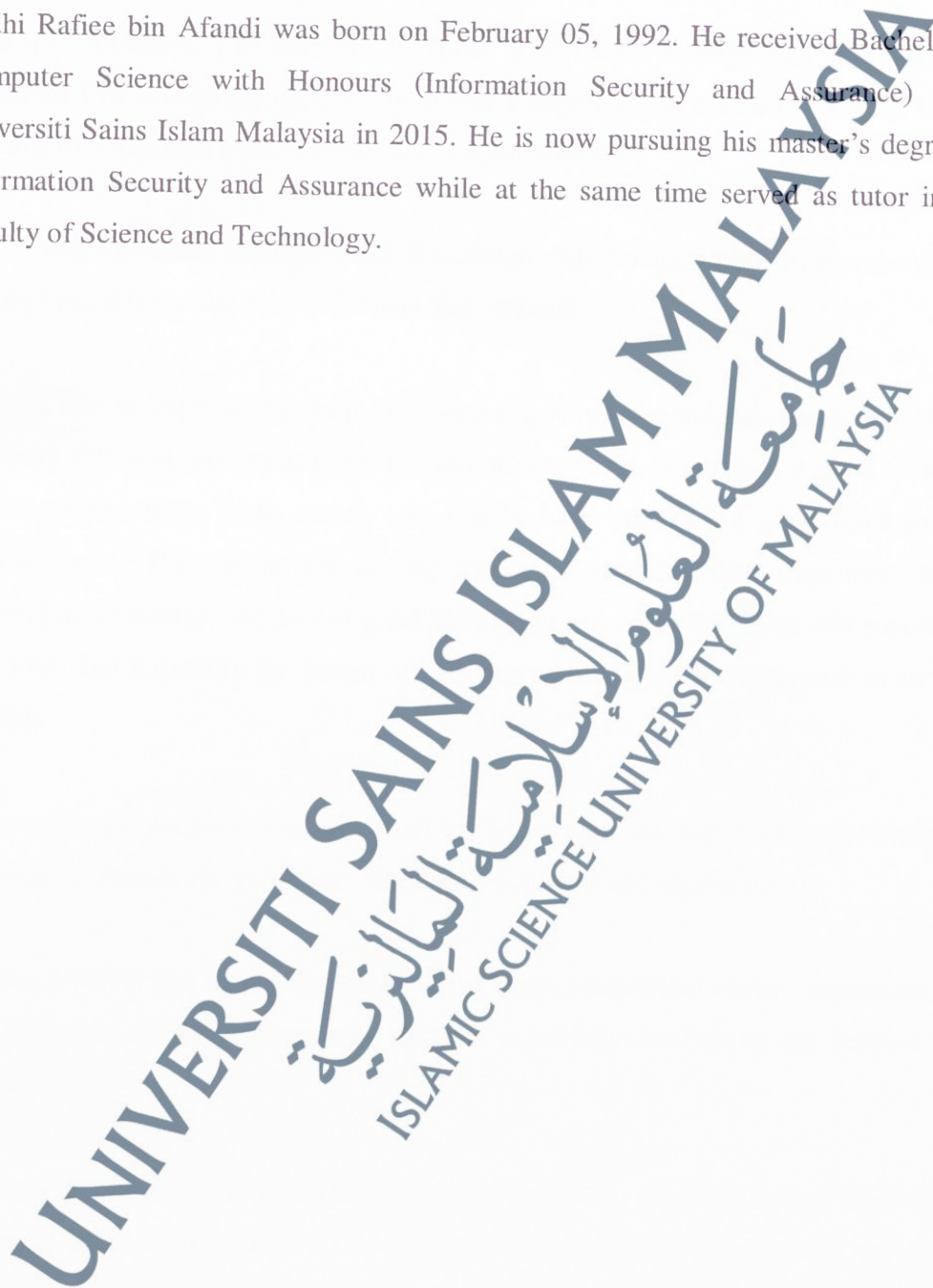
Thesis submitted in fulfillment for the degree of
MASTER OF COMPUTER SCIENCE VIA MIXED-MODE
(INFORMATION SECURITY AND ASSURANCE)

FACULTY OF SCIENCE AND TECHNOLOGY
UNIVERSITI SAINS ISLAM MALAYSIA

December 2016

BIOGRAPHY

Radhi Rafiee bin Afandi was born on February 05, 1992. He received Bachelor of Computer Science with Honours (Information Security and Assurance) from Universiti Sains Islam Malaysia in 2015. He is now pursuing his master's degree in Information Security and Assurance while at the same time served as tutor in the Faculty of Science and Technology.



ACKNOWLEDGEMENTS

First and foremost, I'm thankful to Allah S.W.T that through His Blessings and Guidance I'm able to accomplish my master's degree thesis entitled "ChoCD: Usable and Secure Graphical Password Authentication Scheme".

This thesis dedicated to Afandi bin Ngadiman, Siti Rosmah binti Mohamed, Nadia Nabila binti Afandi and Nadia Natasha binti Afandi.

I would like to express my deep and sincere gratitude to my supervisor, Dr. Mohd Zalisham Jali, with his enthusiasm, inspiration, expertise, patience and great efforts to explain every single thing clearly and simply have provided a good basis for the present thesis. Throughout my writing phase, he provided encouragement, sound advice, good teaching, and lots of good ideas. I pray to Allah S.W.T he will succeed in his career and hopefully his dream of becoming professor will come true as soon as possible.

My sincere appreciation goes out to all of the participants with their contribution in this project. Thanks for your time, feedback, comment and suggestions.

Besides, I would like to say big thanks to my course mates that always supporting me. Not forgotten to all lectures and students especially in Faculty of Science and Technology.

Finally, I would also like to thank Siti Nabilah Basarang, my good friend, who always willing to listen, help and give me continuous encouragement throughout my study. Thanks again to all of you for your cooperation and may Allah bless all of you for your commendable contributories. I pray to Allah SWT to accept this genuine endeavour as a sincere deed.

ABSTRAK

Dalam bidang keselamatan maklumat, pengesahan capaian pengguna adalah topik yang penting untuk dibincangkan. Kata laluan diperkenalkan untuk mengelakkan isu akses tanpa kebenaran, gangguan, pengubahsuaian, pemeriksaan, pendedahan, rakaman atau pemusnahan maklumat. Kata laluan berasaskan teks adalah pengesahan yang terkenal digunakan sejak dari dahulu lagi. Walau bagaimanapun kata laluan berasaskan teks terdedah kepada pelbagai serangan. Pelbagai skim kata laluan grafik telah dicadangkan setakat ini kerana ia dikatakan boleh menangani batasan kata laluan berasaskan teks tersebut. Sejak reka bentuk skim pengesahan kata laluan grafik dikatakan amat penting, kata laluan grafik telah menyediakan kebolehgunaan dan keselamatan yang terbaik untuk pengesahan akses pengguna. Tesis ini bertujuan untuk menangani keperluan dan kekurangan dengan menyediakan reka bentuk baru dan pembangunan skim hibrid yang dinamakan ChoCD. Kaedah kata laluan grafik sebelum ini dikelaskan kepada dua kumpulan: pertamanya adalah berasaskan pengenalanpastian dan keduanya berasaskan pengembalian memori. Berdasarkan tindakan pengguna apabila mereka melakukan pengesahan ke dalam sistem, tesis ini telah mengklasifikasikan pengesahan grafik ke dalam tiga pengesahan grafik; iaitu berasaskan pilihan, berasaskan klik dan berasaskan lukisan corak. Hasil daripada tiga kombinasi kategori itu terhasillah skim hibrid iaitu ChoCD. Dengan hasil gabungan ini, ia dijangka dapat menawarkan kebolehgunaan dan keselamatan secara serentak. Penilaian untuk ChoCD telah dijalankan untuk mengukur kebolehlaksanaan sebagai satu alternatif lain untuk pengesahan akses pengguna. Untuk mendapatkan penilaian yang menyeluruh, ujian ke atas ChoCD dan soal selidik telah dijalankan kepada para peserta. Perbandingan antara ChoCD dan skim pengesahan sedia ada dikenal pasti. Dari penilaian yang telah dilakukan, didapati bahawa ChoCD mudah untuk digunakan dan menyediakan keselamatan yang lebih baik daripada skim yang sedia ada. Justeru itu, penyelidik telah membuktikan bahawa ChoCD mempunyai potensi untuk dilaksanakan dengan lebih meluas pada masa hadapan.

Kata kunci: Kata laluan Grafik, Kata laluan, Keselamatan Pengesahan Pengguna, Kebolehgunaan

ABSTRACT

In the field of information security, user authentication is the vital topic to discuss. Passwords are introduced to prevent unauthorized access, disruption, modification, inspection, disclosure, recording or destruction of information. Text-based password is a well-known authentication used from previous times but text-based passwords are exposed to various attacks such as brute force, guessing, social engineering and dictionary attacks. Various graphical password schemes have been proposed so far as it is said could improve the limitations of password. Since designing effective graphical password authentication schemes is of vital importance, graphical password is said to provide greater usability and security for user authentication. This thesis attempts to address the need by providing a new design and development of hybrid scheme named ChoCD that inspired from users' action namely choice, click and draw. By combining these, it is anticipated that it will offer usability and security simultaneously. An evaluation for ChoCD was conducted to measure its viability for alternative user authentication. To get comprehensive evaluations, the questionnaire has been created and distributed to the participants. The comparisons between ChoCD and existing authentication schemes are identified. From the evaluations conducted, it was found that ChoCD is easy to use and provides better security than other existing schemes. Therefore, the researcher has indicated that ChoCD has potential to be implemented more widely in near future.

Keywords: Graphical Password, Password, User Authentication Security, Usability

مخالصة البحث

في مجال أمن المعلومات، الأثبات الإصالة لدى الشخص هو اهم الموضوع التي تحتاج الى النقاش والمناقشة. قد عرف كلمة السر لأمتناع اي الدخول بدون إذن مثل التشويش والتفتيش والإفشاء والتدمير كل معلومات فيها. كلمة السر التي تستند إلى النص هي الإثبات الإصالة المشهورة منذ الماضي. ولكن هذه الطريقة تكشف من هجمات مثل هجمات القوة الغاشمة وهجمات التخمين وهجمات الهندسة الإجتماعية والقاموس الهجمات. ثم قد اقترح كلمة السر الرسومية المختلفة ليحسن الحديد في كلمة السر نفسها. وبالرغم تصميم كلمة المرور رسومية فعالة ايضا من اهم طريقة لأنها تزود أكبر الإستخدام والضمانة لدى المستخدمين. هذا البحث تحاول أن تهدي الحاجة بتوفير التصميم الجديد وتطوير نظام هجين يسمى ب - سي - إس - أو - سي - دي. هذه كلمة المرور الرسومية السابقة تقسم إلى قسمين : الإعتراض والإستدعاء إذا كان نرجع إلى افعال المستخدمين حينما يوثقون إلى النظام، قد قسم هذا البحث إلى ثلاثة أقسام يسمى بالإختيار والأنقر والرسم. هذه التقسيمات لو نجمع بينهم سيصبح النظام الهجين يسمى ب - سي - إس - أو - سي - دي. هذه المجموعات ستجهز سهولة الإستخدام والضمانة معا. قد صرف التخمين لهذا النظام لكي ان نذرع بقاء لمصادقة المستخدم البديلة. قد انتج ونشر الإستطلاع إلى المشتركين لكي ان يحصل على شمول التقييم. ومن هذا التوزيع ، قد حصل المقارنة بين سي - إس - أو - سي - دي والنظام الموجود في وقتنا الان يعني سي - إس - أو - سي - دي هو أسهل ويوج أكثر ضمان مقارنة بغيره

الكلمة: كلمة السر، كلمة المرور الرسومية ، سهولة ، الأمن المصادقة المستخدم

TABLE OF CONTENT

Contents	Page
TITLE PAGE	
DECLARATION OF THESIS AND COPYRIGHT	i
BIOGRAPHY	ii
ACKNOWLEDGEMENTS	iii
ABSTRAK	iv
ABSTRACT	v
ملخص البحث	vi
TABLE OF CONTENTS	vii
LIST OF TABLES	viii
LIST OF FIGURES	xi
LIST OF APPENDICES	xii
ABBREVIATION/TERMS	xiii
PUBLICATIONS	xiv
1 INTRODUCTION	
1.1 Overview	1
1.2 Background	1
1.3 Problem Statement	3
1.4 Research Questions	4
1.5 Research Objectives	4
1.6 Research Scope	4
1.7 Thesis Structure	5
2 A REVIEW OF GRAPHICAL AUTHENTICATION	
2.1 Overview	7
2.2 Definition	7
2.3 User Authentication Process	8
2.4 Limitations of Text-based Authentication	10
2.5 Overview of Graphical Password Implementation	11
2.5.1 Graphical Authentication	11

2.5.2 Existing Graphical Authentication	14
2.5.3 Existing Hybrid Schemes Authentication	18
2.6 Usability in User Authentication	23
2.7 Graphical Authentication Security	24
2.7.1 Password Entropy	25
2.7.2 Security Attacks in Existing Graphical Password	27
2.8 Summary	30
3 METHODOLOGY	
3.1 Overview	31
3.2 Prototyping Model	31
3.2.1 Development Phases	32
3.3 Development Tools	33
3.4 Combination of Three Graphical Authentications	35
3.4.1 The Illustration of Proposed Graphical Authentication	35
3.5 Method of Evaluation on Password Entropy	37
3.6 Questionnaire Survey	38
3.7 Method of Data Analysis	39
3.8 Summary	40
4 DEVELOPMENT OF ChoCD	
4.1 Overview	41
4.2 The Development of ChoCD	41
4.2.1 Prototype Development by Using Framework	42
4.2.2 Working of Proposed Authentication Scheme	44
4.3 Summary	49
5 ChoCD EVALUATIONS	
5.1 Overview	50
5.2 ChoCD Entropy Evaluation	50
5.2.1 Comparison with Existing Schemes	51
5.3 ChoCD User Testing	52
5.3.1 Background	52

5.3.2 ChoCD Prototype Testing	52
5.4 Results and Analysis	54
5.4.1 Usability Perception Towards ChoCD	56
5.4.2 Security Perception Towards ChoCD	58
5.4.3 Evaluation on ChoCD Authentication Pattern	59
5.4.3.1 Observation for Choice-based phase	60
5.4.3.2 Observation for Click-based and Draw-based phase	61
5.4.4 General Participants' Feedback	64
5.5 Summary	66
6 CONCLUSIONS	
6.1 Overview	68
6.2 Achievements	68
6.3 Limitations	69
6.4 Future Works	70
REFERENCES	72
APPENDICES	78

LIST OF TABLES

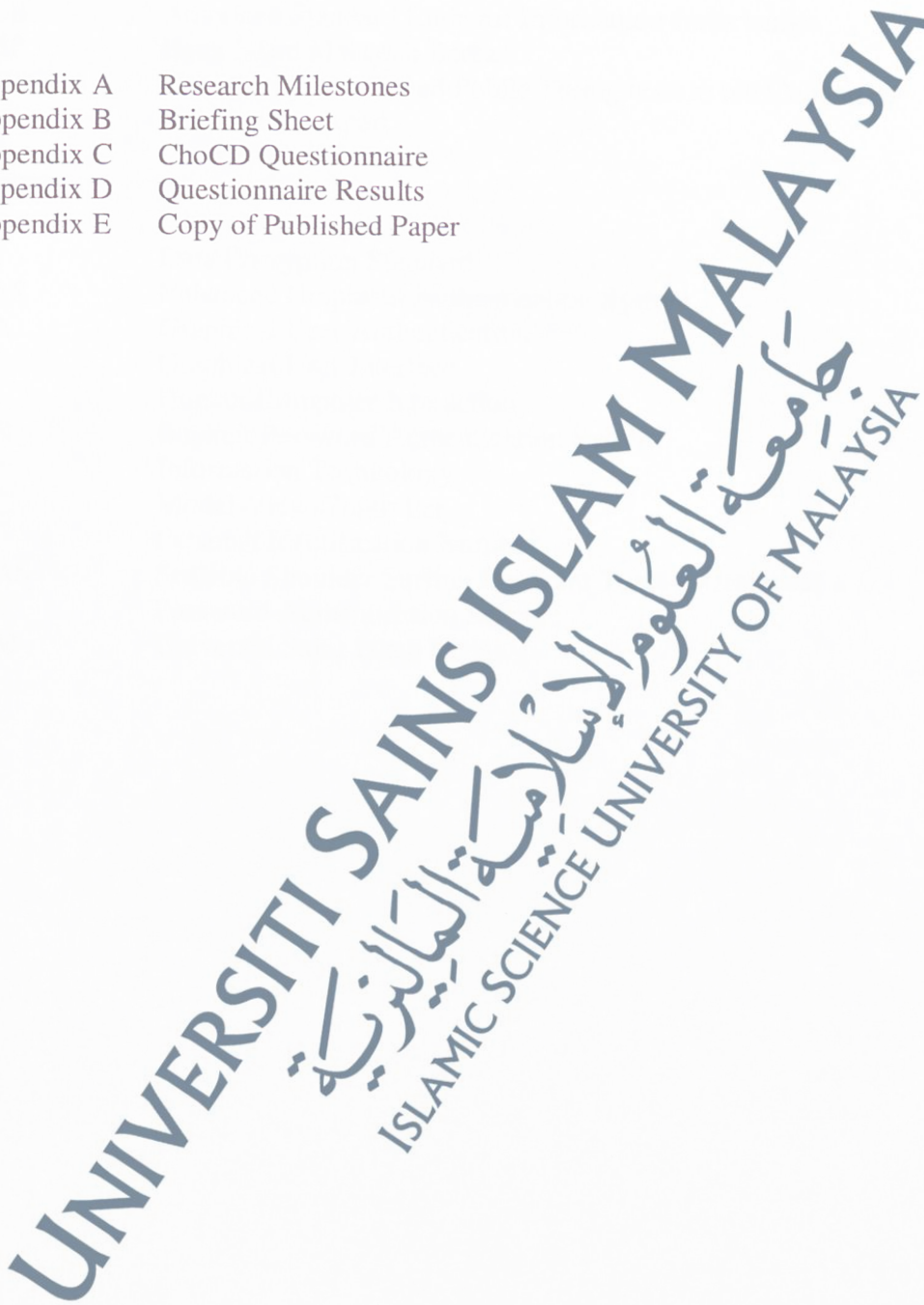
		Page
Table 1.1	Relation of research questions, research objectives and justifications	5
Table 2.1	Image selection in existing graphical authentication scheme	15
Table 2.2	The comparison of usability and security in existing graphical authentication scheme	21
Table 2.3	Password entropy for standard authentication scheme	26
Table 2.4	Password entropy for graphical authentication scheme	27
Table 2.5	The Attack Comparison Based on Three Graphical Password Methods	29
Table 3.1	Software and tools used in the development and testing	34
Table 3.2	Comparison of grid size	38
Table 5.1	Entropy evaluation of ChoCD	51
Table 5.2	Password entropy result between ChoCD and existing authentication scheme	51
Table 5.3	Classification of usability scale by participants	57
Table 5.4	Classification of security scale by participants	59
Table 5.5	Popular images picked by participants	60
Table 5.6	Number of participants for several questions in ChoCD questionnaire	65

LIST OF FIGURES

	Page
Figure 2.1	Group of Graphical Authentication 12
Figure 2.2	Graphical password in Windows 8 16
Figure 2.3	Pattern-draw lock screen in Android 16
Figure 2.4	Confirmation of user authentication in BIMB online banking 17
Figure 2.5	EGAS login interface 19
Figure 2.6	Ray's scheme screenshot 20
Figure 3.1	Prototyping Model 31
Figure 3.2	Mapping from choice-based to click-based and to draw-based 35
Figure 3.3	Initial design of proposed graphical authentication prototype 36
Figure 4.1	Static structure of framework application 42
Figure 4.2	Typical workflow of a framework application 43
Figure 4.3	Flowchart of password creation step 45
Figure 4.4	Flowchart of authentication step 46
Figure 4.5	25 sets of images in 5x5 grid form 47
Figure 4.6	Screenshot of the password creation step 48
Figure 4.7	Screenshot of the authentication step 48
Figure 5.1	No. of participants that contribute in ChoCD questionnaire 55
Figure 5.2	Median time taken in ChoCD process 55
Figure 5.3	Frequency of participants using existing authentication schemes 56
Figure 5.4	The comparison of usability between existing authentication schemes and ChoCD 57
Figure 5.5	The comparison of security between existing authentication schemes and ChoCD 58
Figure 5.6	Samples of clicks and draws made by participants 61
Figure 5.7	Horizontal line 62
Figure 5.8	Horizontal and vertical lines combination 62
Figure 5.9	Horizontal and diagonal lines combination 63
Figure 5.10	Diagonal and vertical lines combination 63

LIST OF APPENDICES

		Page
Appendix A	Research Milestones	78
Appendix B	Briefing Sheet	79
Appendix C	ChoCD Questionnaire	80
Appendix D	Questionnaire Results	81
Appendix E	Copy of Published Paper	83



ABBREVIATIONS/TERMS

ASCII	American Standard Code for Information Interchange
BIMB	Bank Islam Malaysia Berhad
CAPTCHA	Completely Automated Public Turing tests to tell Computers and Humans Apart
CCP	Cued Click Points
ChoCD	Choice-Click-Draw
DAS	Draw-A-Secret
DES	Data Encryption Standard
EGAS	Enhanced Graphical Authentication System
GUA	Graphical User Authentication
GUI	Graphical User Interface
HCI	Human-Computer Interaction
IPAS	Implicit Password Authentication System
IT	Information Technology
MVC	Model-View-Controller
PIN	Personal Identification Number
S3PAS	Scalable Shoulder Surfing Resistant Textual-Graphical Password Authentication Scheme
USIM	Universiti Sains Islam Malaysia

PUBLICATION

The research output and a copy of publication is attached in Appendix E.

- a. Radhi, R. A. & Jali, M. Z. 2017. "ChoCD: Usable and Secure Graphical Password Authentication Scheme". In *2nd International Conference on Recent Trends in Computer Science and Electronics*. 2-3 January 2017, Kuala Lumpur, Malaysia. Published in Indian Journal of Science and Technology (IJST).