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 pengenalpastian 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

مخلصة البحث

في مجال امن المعلومات، الأثبات الإصالة لدى الشخص هو اهم الموضوع التي تحتاج الى النقاش و المناقشة. قد عرف كلمة السرر لأمتناع اي الدخول بدون إذن مثل التشويش و التفتيش و الإفشاء و التدمير كل معلومات فيها. كلمة السرر التي تستند إلى النص هي الإثبات الإصالة المشهورة منذ الماضية. ولكن هذه الطريقة تكشف من هجمات مثل هجمات القوة الغاشمة و هجمات التخمين و هجمات الهندسة الإجتماعية و القاموس 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 و الضمانة لدى المستخدمين. هذا البحث تحاول ان تهدف الحاجة بتوفير التصميم الجديد وتطوير نظام هجين يسمى ب – سي – إش – او – سي – دي. هذه كلمة المرور الرسومية السابقة تقسم إلى قسمين : الإعتراف و الإستدعاء. إذا كان ترجع إلى افعال المستخدمين حينما يوثقون إلى النظام، قد قسم هذا البحث إلى ثلاثة أقسام يسمى بالإختيار و الأنقر و الرسم. هذه التقسيمات لو نجمع بينهم سيصبح النظام الهجين يسمى ب - سي – إش – او – سي – دي. هذه المجموعات ستجهز سهولة الإستخدام و الضمانة معا. قد صرف التخمين لهذا النظام لكي ان نذرع بقاءه لمصادقة المستخدم البديلة. قد انتج ونشر الإستطلاع إلى المشتركين لكي ان يحصل على شمول التقييم. ومن هذا التوزيع ، قد حصل المقارنة بين سي – إش – او – سي – دي و النظام الموجود في وقتنا الان يعني سي – إش – او – سي – دي هو اسهل ويوج اكثر ضمان مقارنة بغيره

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

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

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).