SECURE APPRECIATIVE INQUIRY FUZZY QUANTIFICATION TECHNIQUE FOR QUANTIFYING SOFTWARE SECURITY REQUIREMENTS

Omar Isam Homaidi Al Mrayat

(Matric No. 4110194)

Thesis submitted in fulfillment for the degree of

DOCTOR OF PHILOSOPHY

IN

SCIENCE AND TECHNOLOGY

(COMPUTER SCIENCE)

Faculty of Science and Technology

UNIVERSITI SAINS ISLAM MALAYSIA

NILAI

January 2015

AUTHOR DECLARATION

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

Date: 18th January 2015 Signature :

Name : Omar Isam al-mrayat.

Matric No : 4110194

Address : P13-A-08-02 SRI Cempaka Apartment Jalan Sepakat Indah 2, Kajang Selangor

BIODATA OF AUTHOR

Omar Isam Homaidi AL- Mrayat is pursuing his PhD from faculty of Science and Technlogy, Universiti Sains Islam Malaysia with matric no 4110194. He is Jordanian with passport no L029169 and currently resides at Amman, Jordan. He obtained a Master in Computer and Network Security from New York Institute of Technology (NYIT), USA. His research interest includes Software Engineering, Requirements Engineering, Requirements Elicitation, Fuzzy Soft Set Theory, and Security Requirements Engineering. Contact: Email: omar_sql@yahoo.com

ACKNOWLEDGEMENT

This thesis was not by any means a solo effort. It's my pleasure to convey my gratitude to them all in my humble acknowledgment.

Foremost, I would like to express my sincere gratitude to my advisors Prof Dr Norita Md Norwawi and Dr.Nurlida Binti Basir for the continuous support of my Ph.D study and research, for their patience, motivation, enthusiasm, and immense knowledge. Their guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisors and mentors for my Ph.D study.

Last but not the least, I would like to thank my family: my wife wafaa for her patience, motivation, enthusiasm and supporting, my parents Isam and Sahar, for giving birth to me at the first place and supporting me spiritually throughout my life.

ABSTRAK

Pembangun perisian umumnya memfokuskan kepada fungsi utama dan ciri-ciri asas sistem di mana aspek keselamatan ditumpukan di fasa penghujung dan lewat. Keperluan keselamatan yang kurang diberi perhatian di fasa awal pembangunan boleh menyebabkan perisian yang lemah ciri keselamatan serta melibatkan kos yang berlipat ganda tinggi untuk dibaiki disetiap fasa. Menilai tahap keselamatan perisian di fasa awal pembangunan sistem membantu menghasilkan rekabentuk. aplikasi yang selamat serta berupaya melindungi dari serangan yang bertujuan untuk merosak. Oleh itu pembangun sistem dan perisian perlukan pendekatan yang praktikal dan sistematik untuk mendapatkan maklumat yang cukup dan berkredibiliti ke atas tahap keselamatan sistem yang sedang dibangunkan di fasa awal kitaran pembangunan perisian. Setakat ini teknik yang bolehpercaya dan kukuh atau kaedah mengukur secara kuantitatif keperluan keselamatan dalam industri perisian sangat terhad. Oleh itu, tujuan kajian ini adalah untuk membina satu kerangka kerja untuk memperoleh keperluan keselamatan dan mengkuantifikasikan keperluan keselamatan untuk memastikan perisian yang selamat dibangunkan. Usul satu kerangka kerja yang dipanggil *Secure Appreciative Inquiry Fuzzy Quantification Technique (SAIFQT)* dengan mengintegrasikan teknik-teknik *Appreciative Inquiry*, *SQUARE*, *CLASP* and *Fuzzy Soft Set Theory* untuk memperoleh keperluan sistem beserta pengukuran kuantitatif. Diakhir kajian, penilaian ke atas teknik SAIFQT melalui kajian kes sebenar, ujian penetrasi dan pengesahan oleh pakar bidang keselamatan secara heuristik dilaksanakan ke atas prototaip yang dibina. *Mix Method* dengan gabungan kaedah kualitatif dan exploratif digunakan. Kajian ini membuktikan kerangka kerja yang dicadangkan *SAIFQT* dibuktikan berjaya untuk memperoleh spesifikasi keperluan keselamatan yang baru dan unik. Dapatan menunjukkan kekuatan pada kerangka yang diusulkan dibandingkan dengan kaedah normal SDLC berdasarkan laporan keputusan ujian penetrasi yang menggariskan tiga prioriti tahap rendah amaran keselamatan. Manakala laporan ujian ke atas prototaip yang dibangunkan menggunakan kaedah SAIFQT menunjukkan empat prioriti tahap tinggi amaran keselamatan, satu untuk tahap sederhana, satu untuk tahap rendah dan prioriti bermaklumat. Oleh itu kajian ini melaporkan sumbangan kerangka ini meliputi kelonggaran atau *vulnerability* keselamatan perisian yang akan dibangunkan di masa akan datang.

ABSTRACT

Software developers generally focused on the core's functions and features, but the security was only addressed as an afterthought even though it was too late. The lack of proper consideration of security requirements during the early stages may lead to the development of an application with a poor security and the cost of correcting it might increase several times with every additional developmental phase. Assessing security at an early stage helps to design a secure application that can withstand malicious attacks. Therefore, software and system developers need practical and systematic approaches to obtain sufficient and credible evidence of the security level in the system, which is under development in the early phases of software development life-cycle (SDLC). Currently, there is limited number of reliable technique or method to quantify security requirements in software industry. Thus, the objective of the study is to construct a framework to elicit and quantify security requirements in order to ensure secure software been developed. Here, the work introduce a framework called Secure Appreciative Inquiry Fuzzy Quantification Technique (SAIFQT) which integrate Appreciative Inquiry, SQUARE, CLASP and Fuzzy Soft Set Theory techniques in eliciting and quantifying security requirements. The proposed framework, SAIFQT was evaluated with by case studies, penetration testing and validated by security experts. A mixed methodology was used in this study, a qualitative and explorative method. The results show that the proposed technique, SAIFQT was proved successfully in eliciting a new and unique software and security requirements specification. The results show the strong points in the proposed technique comparing to the normal SDLC, according to penetration testing reports, which shows three low priority alerts for the proposed technique. Meanwhile the report related to the prototype built using normal SDLC shows four high priority alerts and one for each of medium, low and informational priority security alerts. Thus, this study registered their contribution to cover security vulnerability in software intended to be build in future.

ملخص

مطورين البرمجيات يركزون بشكل عام على المتطلبات الأساسية للنظام، ولكن ما يخص المسائل الأمنية تضاف في وقت متأخر للنظام. أن عدم الاهتمام بأضافة المتطلبات الأمنية في مراحل مبكرة في تصنيع النظام يؤدي إلى تسليم نظام ضعيف ومليء بالثغرات يكلف تصليحها مستقبلاً أضعاف مضاعفة من تكاليف البرنامج الأصلية. توظيف العناصر الأمنية في مراحل مبكرة يزود المستفيدين بنظام آمن ومتصدي للهجمات. لذلك فإن مطوري البرمجيات بحاجة ماسة إلى أدوات وطرق تعزز وتمنح حالة ومستوى الأمن عند اصناعة البرمجيات وخاصة في مراحل مبكرة من دورة حياة البرنامج (SDLC). في الوقت الحالي هناك عدد محدود من التقنيات والطرق التي يتم الأعتماد عليها في تزويد كم هو النظام آمن قبل أن يكتمل بناءه. لذلك تهدف هذه الدراسة إلى بناء تقنية تقوم بتزويد المتطلبات الأمنية المتعلقة بالنظام لظمان تزويد المستخدمين بأنظمة آمنة. ومن هنا فإن الدراسة تزود تقنية تدعى "تقنية التقدير الكمي الضبابي الآمن (SAIFQT). لقد تم تقييم التقنية المقترحة باستخدام حالات دراسة وتقنية الإختراق وتم التأكد من صحة التقنية المقترحة بوساطة خبراء الأمن. منهجية الجودة والطريقة الاستعراضية استخدمت في هذه الدراسة. أظهرت النتائج ان التقنية المقترحة (SAIFQT) قد أثبتت نجاحها في استنباط متطلبات أمنية جديدة وفريد من نوعها إلى جانب ذلك استخلاص المتطلبات الأمنية لأي نظام منويّ إنشائه كمياً وقبل بناءه وتسليمه وليس بعد وذلك باستخدام القليل من دراسات الحالة. أظهرت النتائج النقاط القوية في التقنية المقترحة بالمقارنة مع (SDLC) العادية، والتي غطت الكثير من الثغرات الأمنية التي لم تستطع (SDLC) العادية تغطيتها بناءً على تقارير الإختراق التي أظهرت ثلاثة تنبيهات منخفضة الأولوية للتقنية المقترحة في حين أن التقارير أظهرت أربعة تنبيهات عالية الأولوية وواحد لكل من متوسط ومنخفض ومعلوماتي التنبيه فيما يتعلق بالنموذج المبدئي الذي صمم باستخدام (SDLC) العادية. لذلك سجلت هذه الدراسة مساهمتها العلمية لتغطية أي ثغرات أمنية في أي نظام مرجو بنائه مستقبلاً.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

AI	Appreciative Inquiry
CIA	Confidentiality, Integrity and Availability
CLASP	Comprehensive, Lightweight Application Security Process
CREE	Confidentiality Requirements Elicitation and Engineering
EI	Errors Index
MSRA	Multilateral Security Requirements Analysis
RE	Requirements Engineering
SAIFQT	Secure Appreciative Inquiry Fuzzy Quantification Technique
SAIT	Secure Appreciative Inquiry Technique
SDLC	Software Development Life Cycle
SE	Software Engineering
SI	Security Index
SQUARE	Security Quality Requirements Engineering
SR	Security Requirements
SRE	Security Requirements Engineering
SRI	Security Requirements Index
STEP	Software Test and Evaluation Panel
UML	Unified Modeling Language
VI	Vulnerabilities Index
XP	Extreme Programming