



**UNIVERSITI PUTRA MALAYSIA**

**COST ESTIMATION MODEL FOR SECURE SOFTWARE DEVELOPMENT**

**NUR ATIQA SIA ABDULLAH @ SIA SZE YIENG**

**FSKTM 2011 11**

**COST ESTIMATION MODEL FOR SECURE  
SOFTWARE DEVELOPMENT**

**By**

**NUR ATIQA H SIA ABDULLAH @ SIA SZE YIENG**

**Thesis Submitted to the School of Graduate Studies, Universiti Putra  
Malaysia, in Fulfilment of the Requirements for the Degree of  
Doctor of Philosophy**

**August 2011**

## DEDICATION

I want to dedicate this work to my beloved husband, Syed Mohd Ifandi Syed Jaafar, my two lovely daughters, Sharifah Nur Syuhada dan Sharifah Nur Syahadah, and my parents Joseph Sia Ming Moi and Chiong Siew Ding.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment  
of the requirement for the degree of Doctor of Philosophy

**COST ESTIMATION MODEL FOR SECURE  
SOFTWARE DEVELOPMENT**

By

**NUR ATIQAHA SIA ABDULLAH @ SIA SZE YIENG**

**August 2011**

**Chair: Associate Professor Rusli bin Abdullah, PhD**

**Faculty: Faculty of Computer Science and Information Technology**

Engineering security in software is now a high priority objective in many IS application especially for the banking and electronic commerce. Most of the commerce websites are forced to add on security coding to prevent them from web criminal. These are due to the poor coding and lacking in considering security during system development life cycle (SDLC). To build security into the applications or systems, it will substantially raise software costs. The existing software cost estimation (SCE) models are lacking in emphasis on the security coding or factors in estimating the software cost. Therefore, there is a need to have cost estimation model for the secured software in order to have more accurate estimation.

Some of the researchers have tried to extend COCOMO II by including security cost drivers. In this thesis, however, due to the security issues highlighted by Function Point Analysis (FPA), a Software Security Characteristics Model (SSCM) is proposed to be extended in the FPA to include the security costing.

To produce SSCM, two software security measurement metrics, which are Davis's software security management and metric; and McGraw's software security seven touch points, are considered to derive the security aspects according to SDLC. The security aspects are then cross-referenced with four common security standards. These standards include Information Technology (IT) Security Cost Estimation Guide, Common Criteria for Information Technology Security Evaluation, Open Web Application Security Project (OWASP), and Control Objectives for Information and related Technology (COBIT). These characteristics are then arranged according to the security aspects. As a result, SSCM, which consists of 48 characteristics, is developed.

To validate the model, a survey is setup to investigate the current practices in Multimedia Super Corridor (MSC) software houses in Klang Valley, Malaysia. The survey results are analyzed using Rasch Measurement Method. The results reveal a person spread of  $5.52logit$  with good Separation,  $G=3.64$  and excellent Reliability of  $Cronbach-\alpha = 0.97$ , which means the survey outcome is acceptable. With  $\mu_{person}$  of  $83.06\%$  and the Person Mean =  $1.59 \geq 0.00$ ; with significant of  $p=0.05$ , the SSCM are valid, relevant and implemented in current practices.

This validated SSCM is then corroborated through expert opinions in verifying the discarded characteristics. The final SSCM is used to extend the General System Characteristics (GSCs) in FPA by including two additional evaluation sheets, which are specified in calculating the security costing. The evaluation score for these sheets is based on the result of Rasch in the survey.

An online estimation tool is developed based on the SSCM and so called Extended FPA in an experiment. To evaluate the user acceptance towards this tool, a user acceptance model has been adapted based on three theoretical models, which are Technology Acceptance Model (TAM), Method Evaluation Model (MEM) and Part 3 ISO/IEC 14143 (ISO/IEC). This adapted model is the basic for the user acceptance questionnaire and hypotheses in the laboratory experiment. Besides, case studies are designed as experiment materials. This experiment is then carried out to test the user acceptance towards the Extended FPA compared to the IFPUG FPA. The respondents are trained with both FSM methods according to within-subject design. There are comparative analyses between two FSM methods in this experiment. From the user acceptance results, we can concluded that seven out of nine null hypotheses are rejected, which shows overall the responses to the post-task surveys suggested that Extended FPA is more consistent, easier to use, more useful and nevertheless is more likely to be used in the future.

As a conclusion, the results of this study are contributed in theoretical and practical aspect. For the theoretical aspect, several models and theories are integrated in a systematic way: SSCM, Research Design, and Empirical Studies.; while for the practical aspect, this study deals with current problem in the industry: the security costing for the secure software.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk Ijazah Doktor Falsafah

**MODEL ANGGARAN KOS UNTUK PEMBANGUNAN  
KESELAMATAN DALAM PERISIAN**

Oleh

**NUR ATIQAH SIA ABDULLAH @ SIA SZE YIENG**

**Ogos 2011**

**Pengerusi: Profesor Madya Rusli bin Abdullah, PhD**

**Fakulti: Fakulti Sains Komputer dan Teknologi Maklumat**

Kejuruteraan keselamatan dalam perisian kini menjadi objektif utama dalam kebanyakan perisian terutamanya bagi perbankan dan perdagangan elektronik. Kebanyakan laman dagang terpaksa menambah kod keselamatan untuk menghindari daripada jenayah web. Ini adalah disebabkan oleh kekurangan kod keselamatan dan keprihatinan tentang keselamatan perisian semasa kitar hayat pembangunan sistem (SDLC). Untuk membina keselamatan ke dalam aplikasi atau sistem, ini semestinya akan meningkatkan kos perisian. Model anggaran kos perisian (SCE) yang sedia ada kurang menekankan kepada kod atau faktor keselamatan dalam menganggarkan kos perisian. Oleh itu, terdapat keperluan mewujudkan model anggaran kos untuk pembangunan keselamatan dalam perisian agar dapat membuat anggaran yang lebih tepat.

Beberapa penyelidik telah cuba untuk melanjutkan COCOMO II dengan memasukkan pemacu kos keselamatan. Walau bagaimanapun, dalam tesis ini, disebabkan isu-isu keselamatan yang diketengahkan oleh Analisis Fungsian Poin

(FPA), Model Ciri Keselamatan Perisian (SSCM) adalah dicadangkan untuk diperluaskan dalam FPA bagi merangkumi kos keselamatan.

Untuk menghasilkan SSCM, dua metrik perisian pengukuran keselamatan, iaitu pengurusan dan metrik keselamatan perisian Davis; dan tujuh titik sentuh keselamatan perisian McGraw, telah dipertimbangkan untuk memperolehi aspek-aspek keselamatan mengikut SDLC. Aspek-aspek keselamatan kemudiannya saling rujuk dengan empat piawaian keselamatan biasa. Piawaian ini termasuklah Teknologi Maklumat (IT) Panduan Anggaran Kos Keselamatan, Common Criteria bagi Penilaian Keselamatan Teknologi Maklumat, Projek Keselamatan Aplikasi Laman Terbuka (OWASP), dan Objektif Kawalan bagi Maklumat dan Berkaitan dengan Teknologi (COBIT). Ciri-ciri ini kemudiannya disusun mengikut aspek-aspek keselamatan. Hasilnya, SSCM, yang terdiri daripada 48 ciri, telah dibangunkan.

Untuk mengesahkan model, satu kaji selidik dijalankan untuk menyiasat amalan semasa syarikat perisian Koridor Raya Multimedia (MSC) di Lembah Klang, Malaysia. Keputusan kaji selidik telah dianalisis menggunakan Kaedah Pengukuran Rasch. Keputusan mendedahkan penyebaran orang  $5.52logit$  dengan Pemisahan baik,  $G = 3,64$  dan Kebolehpercayaan hebat daripada  $Cronbach-\alpha = 0.97$ , yang bermaksud hasil kaji selidik yang boleh diterimapakai. Dengan  $\mu_{person} 83,06\%$  dan  $Min Responden = 1,59 \geq 0,00$ ; dengan signifikan  $p = 0.05$ , SSCM adalah sah, relevan dan yang dilaksanakan dalam amalan semasa.



SSCM yang telah disahkan kemudiannya disokong melalui pendapat pakar dalam mengesahkan ciri-ciri yang perlu disingkirkan. SSCM yang terakhir adalah digunakan untuk menambah Ciri-ciri Sistem Am (GSCs) di FPA termasuklah dua lembaran penilaian tambahan yang dinyatakan dalam mengira kos keselamatan. Skor penilaian lembaran ini adalah berdasarkan hasil Rasch dalam kaji selidik.

Satu aplikasi anggaran dalam talian telah dibangunkan berdasarkan SSCM dan dirujuk sebagai *Extended FPA* dalam ujikaji. Untuk menilai penerimaan pengguna terhadap aplikasi ini, model penerimaan pengguna telah disesuaikan berdasarkan tiga model teori, iaitu Model Penerimaan Teknologi (TAM), Kaedah Model Penilaian (MEM) dan Bahagian 3 ISO / IEC 14143 (ISO / IEC). Model yang diubahsuai ini merupakan asas kepada soal selidik penerimaan pengguna dan hipotesis dalam ujikaji. Selain itu, kajian kes telah direka sebagai bahan ujikaji. Ujikaji ini dijalankan untuk menguji penerimaan pengguna ke arah FPA Extended berbanding FPA IFPUG. Responden telah dilatih dengan kedua-dua kaedah FSM mengikut reka bentuk dalam-subjek. Terdapat analisis perbandingan antara dua kaedah FSM dalam ujikaji ini. Daripada keputusan penerimaan pengguna, kita boleh menyimpulkan bahawa tujuh daripada sembilan hipotesis telah ditolak, ini menunjukkan keseluruhan jawapan kepada kaji selidik selepas tugas yang disyorkan bahawa *Extended FPA* lebih konsisten, lebih mudah untuk digunakan, lebih berguna dan lebih cenderung untuk digunakan pada masa hadapan.

Sebagai kesimpulan, keputusan kajian ini menyumbang dalam aspek teori dan praktikal. Bagi aspek teori, beberapa model dan teori yang bersepadu dalam cara yang sistematik:. SSCM, Reka Bentuk Penyelidikan dan Kajian Empirical, manakala

bagi aspek praktikal, ini tawaran belajar dengan masalah semasa dalam industri:  
keselamatan yang bernilai untuk perisian selamat.



## ACKNOWLEDGEMENTS

First of all, I would like to thank Allah s.w.t for giving me the spiritual strength to finish this study. Besides, I would like to express my special thank to my main supervisor, Assoc. Prof. Dr Rusli Abdullah for his fully support and encouragement during the study. I would also like to give my special thanks to Assoc. Prof. Hj. Mohd Hasan Selamat on his valuable critiques that brought a great influence on this study. I am also very grateful to Assoc. Prof. Dr. Azmi Jaafar for giving me lot guidance during the data analysis and results in this study.

I would like to give my special thanks to Mohd Faisal Ibrahim for guiding me during the preparation of VIVA and Norzilah Musa for supporting me spiritually. I would like to express my sincere appreciation to Mr Mohd Saidfudin Masodi for giving me professional consultancy on the performance measurement (Rasch model). His expertise helped me to complete the survey, data analysis and discussion. Besides, I would like to thank all the people who were willing to participate during the survey, expert opinions, and laboratory experiment. The important parts of this study would not have been possible without the participation and cooperation of these people. Special thanks to Mr. Peter Sia Chin Yong for working with me and contributed ideas in developing the online estimation tool in this study.

Thanks to all the PhD and Master's friends that provided me useful materials and references on the theoretical and empirical validation of software metrics and user acceptance models. Also thanks to the staffs for all their help and support during my study in Universiti Putra Malaysia. Thanks to Ministry of Higher Education

(Malaysia) and Universiti Teknologi MARA (UiTM) for financially supporting this study.

I want to give very special thanks to my husband, Syed Mohd Ifandi Syed Jaafar, for his love, support and encouragement throughout this study. Also thanks to my lovely daughters, Sharifah Nur Syuhada and Sharifah Nur Syahadah, for accompanying me all the nights I spent writing this thesis. Thanks to my dearest sister, Mary Sia Sze Hung, for being the babysitter for my daughters during the school holidays. Gratitude to my best friend, Kartini Rashid, who is always be my side regardless the worst or best situation. Last but not least, I have to thank my parents, Joseph Sia Ming Moi and Chiong Siew Ding, for giving me their fully loves and cares.

**NUR ATIQAH SIA ABDULLAH @ SIA SZE YIENG**

**August 2011**

I certify that a Thesis Examination Committee has met on 12 August 2011 to conduct the final examination of Nur Atiqah Sia Abdullah on her thesis entitled “Cost Estimation Model for Secure Software Development” in accordance with the Universities and University College Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

**Zuriati binti Ahmad Zulkarnain, PhD**

Associate Professor  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Chairman)

**Abdul Azim bin Abd Ghani, PhD**

Professor  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Internal Examiner)

**Rodziah binti Atan, PhD**

Associate Professor  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Internal Examiner)

**Richard Lai, PhD**

Associate Professor  
Faculty of Science, Technology and Engineering  
La Trobe University  
Victoria, Australia  
(External Examiner)

---

**NORITAH OMAR, PhD**

Associate Professor and Deputy Dean  
School of Graduate Studies  
Universiti Putra Malaysia

Date: 28 October 2011

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

**Rusli bin Abdullah, PhD**

Associate Professor  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Chairman)

**Mohd Hasan bin Selamat, MPhi.**

Associate Professor  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Member)

**Azmi bin Jaafar, PhD**

Associate Professor  
Faculty of Computer Science and Information Technology  
Universiti Putra Malaysia  
(Member)

---

**HASANAH MOHD. GHAZALI, PhD**

Professor and Dean  
School of Graduate Studies  
Universiti Putra Malaysia

Date:

## DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or at any other institution.

---

**NUR ATIQAHA SIA ABDULLAH @ SIA SZE YIENG**

Date: 12 August 2011

## TABLE OF CONTENTS

	<b>Page</b>
<b>DEDICATION</b>	ii
<b>ABSTRACT</b>	iii
<b>ABSTRAK</b>	vi
<b>ACKNOWLEDGEMENTS</b>	x
<b>APPROVAL</b>	xii
<b>DECLARATION</b>	xiv
<b>LIST OF TABLES</b>	xix
<b>LIST OF FIGURES</b>	xxi
<b>LIST OF APPENDICES</b>	xxiii
<b>LIST OF ABBREVIATIONS</b>	xxiv
<b>CHAPTER</b>	
<b>1 INTRODUCTION</b>	<b>1</b>
1.1 Background	1
1.2 Problem Statements	2
1.3 Research Questions	5
1.4 Research Objectives	6
1.5 Research Scopes	7
1.6 Research Methodology	8
1.7 Importance of Study	9
1.8 Organization of Thesis	10
<b>2 LITERATURE REVIEW</b>	<b>12</b>
2.1 Introduction	12
2.2 Software Measurement	12
2.3 Measurement Approaches	13
2.4 Types of Software Measure	13
2.4.1 Software Size Measures	15
2.4.2 Measurement Scales	16
2.5 Application of Software Measurement	18
2.6 Function Point Measure	19
2.7 Function Point Analysis	20
2.7.1 Function Point Components	21
2.7.2 Function Point Complexity Weights	22
2.7.3 Function Point General System Characteristics	23
2.7.4 Function Point Counting Procedure	25
2.7.5 Function Point Applications	26
2.8 Extended Function Point Analysis Techniques	27
2.8.1 Feature Points	27
2.8.2 Mark II Function Point and Model	28
2.8.3 3D Function Point	31
2.8.4 Full Function Point	32
2.8.5 COSMIC Full Function Point	32



2.9	Other Parametric Cost Estimation Techniques	33
2.9.1	Putnam's SLIM	33
2.9.2	Boehm's COCOMO II	34
2.9.3	Banker's Object Point	36
2.9.4	Cleary's Web Point	37
2.9.5	Component Point	38
2.10	Limitations of Cost Estimation Models	41
2.10.1	Security Cost and Its Effect on Software Cost Estimation	41
2.10.2	Extension of COCOMO II with Security Concerns	43
2.10.2.1	COSECMO	43
2.10.2.2	Security Cost Driver	46
2.10.2.3	Security Risk Analysis	48
2.10.3	Evaluation of Cost Estimation Models with Security Concern	49
2.11	Software Security Measurement Metrics	52
2.11.1	Software Security Management and Metric	53
2.11.2	McGraw's Software Security Seven Touch Points	53
2.12	Common Security Standards	55
2.12.1	Information Technology Security Cost Estimation Guide	55
2.12.2	Common Criteria for Information Technology Security Evaluation	57
2.12.3	The Open Web Application Security Project	58
2.12.4	Control Objectives for Information and related Technology	59
2.13	Summary	60
3	<b>RESEARCH METHODOLOGY</b>	62
3.1	Introduction	62
3.2	Research Methodology Description	62
3.3	Software Security Characteristics Selection	64
3.4	Instrument Construct for Survey	65
3.4.1	Objective	66
3.4.2	Hypothesis	66
3.4.3	Sampling	67
3.4.4	Measurement Instrument Setting	68
3.4.5	Data Collection for Survey	69
3.5	Rasch Analysis Method	69
3.5.1	Person-Item Distribution Map	71
3.5.2	Person Validity	72
3.5.3	Items Validity and Suspected Items Identification	72
3.5.4	Category Structure	73
3.5.5	Ability Calculation	73
3.6	Expert Opinions	74
3.7	Experiment Construct	75
3.7.1	Theoretical Models for User Acceptance	77
3.7.1.1	The Technology Acceptance Model (TAM)	77
3.7.1.2	The Method Evaluation Model (MEM)	78
3.7.1.3	ISO/SEC 14143-3 Information technology – Software measurement – Functional size measurement	80

3.7.2	Adaptation of TAM, MEM and ISO/IEC in User Acceptance Models	82
3.7.3	Questions for User Acceptance Questionnaire	84
3.7.4	Experiment Research Questions	85
3.7.5	Variable Selection	86
3.7.6	Hypotheses Formulation	88
3.7.7	Comparative Evaluation of Extended FPA against IFPUG FPA	89
3.7.8	Selection of Subjects	93
3.7.9	Software Specification Requirements	93
3.7.10	Experiment Treatments	95
3.7.11	Experiment Operations	98
3.8	Summary	101
<b>4</b>	<b>MODEL DESIGN AND DEVELOPMENT</b>	<b>106</b>
4.1	Introduction	106
4.2	Software Security Characteristics Model Design	106
4.2.1	Integration for Software Security Measurement Metrics	107
4.2.2	Cross-reference Common Security Standards	109
4.2.3	Organization of Software Security Characteristics in SDLC	110
4.3	Extension of General System Characteristics	112
4.3.1	Software Security Characteristics as General System Characteristics	112
4.3.2	Degree of Influence	113
4.3.3	Calculation in General System Characteristics	115
4.4	System Design	116
4.4.1	System Specification	116
4.4.2	System Architecture	118
4.4.3	Modeling Process	119
4.4.3.1	Context Diagram	119
4.4.3.2	Decomposition Diagram	120
4.4.3.3	Data Flow Diagram	121
4.4.3.4	Entity Relationship Diagram	122
4.4.4	System Interfaces	123
4.5	Summary	127
<b>5</b>	<b>RESULTS AND DISCUSSION</b>	<b>128</b>
5.1	Introduction	128
5.2	Survey Analysis	128
5.2.1	Respondents Profile	129
5.2.2	Person-Item Distribution Map	131
5.2.3	Summary Statistics for Person and Item Measure	133
5.2.4	Person Measure Analysis	134
5.2.5	Item Measure Analysis	136
5.2.6	Item Polarity	138
5.2.7	Category Structure Calibration	140
5.2.8	Awareness for Security Characteristics	142
5.3	Expert Opinions Analysis	143

5.4	User Acceptance Testing Analysis	144
5.4.1	Comparative Analysis of the Performance of the FSM Methods	144
5.4.2	Comparative Analysis of the Likelihood of Adoption in Practice of the FSM Methods	148
5.4.3	Analysis of the Acceptance of the Extended FPA	152
5.5	Threat Validity	154
5.6	Summary	156
<b>6</b>	<b>CONCLUSIONS AND FUTURE WORKS</b>	<b>158</b>
6.1	Introduction	158
6.2	Conclusions	158
6.2.1	Design of the Software Security Characteristics	158
6.2.2	Validation of the Software Security Characteristics Model	159
6.2.3	Design a Tool to Analyze the Software Security Costing	160
6.2.4	Validation of the Application of the Extended FPA in Experiment	161
6.2.5	Summary of the Main Contributions	162
6.3	Future Works	163
	<b>REFERENCES</b>	<b>164</b>
	<b>APPENDICES</b>	<b>171</b>
	<b>BIODATA OF STUDENT</b>	<b>220</b>
	<b>LIST OF PUBLICATIONS</b>	<b>221</b>