

**SYSTEMATIC SECURE DESIGN GUIDELINE TO IMPROVE INTEGRITY AND
AVAILABILITY OF SYSTEM SECURITY**

ASHVINI DEVI A/P KRISHNAN

A dissertation submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Science (Computer Science)

Faculty of Computing
Universiti Teknologi Malaysia

OCTOBER 2013

I declare that this dissertation entitled “*Systematic Secure Design Guideline To Improve Integrity And Availability Of System Security*” is the result of my own research except as cited in the references. The dissertation has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature :

Name : Ashvini Devi A/P Krishnan

Date : October 18, 2013

This dissertation is dedicated especially to my beloved mother, Mrs. Gunasundari and father, Mr. Krishnan and also not forgetting my beloved siblings for their endless supports and encouragements.

ACKNOWLEDGEMENT

First and foremost, I would like to express my utmost gratitude to God for endless blessings and given me strength to during the development of this research until it has completed.

I am also heartily grateful and thankful to my supervisor **Dr. Dayang Norhayati Abang Jawawi** for her constant supports during my study at UTM. She has inspired me greatly to work in this Dissertation. Her motivations and guidance have contributed tremendously in completing the research. I have learned a lot from her and I am fortunate to have her as my mentor and supervisor.

Besides, I would like to thank the authority of Universiti Technologi Malaysia (UTM) for providing me with a good environment and facilities during my stay in UTM.

ABSTRACT

Security is the most important dimension to the systems that involves processing and interchange of confidential information. Therefore it is a must to be designed so that they achieved a high level at security. Security specification languages can be used to represent security specification such as attack specification or to be more precise about who can do what and when, and this can be achieved by enforcing access control. The suitable approach to enforce access control is Role-Based Access Control (RBAC). Only secureUML metamodel is using RBAC as security mechanism. However, secureUML metamodel does not indicate the properties of supporting basic security requirements which focusing on integrity and availability, and even the consideration of situation that leads to different possible attacks. The objective of this dissertation is to propose a systematic secure design guideline by enhancing secureUML metamodel. The enhancement is performed by integrating with protection-levels of secured layers which provides protection for the critical assets in various layers to support integrity and availability and to identify possible internal threats based on scenario by using Step-by-Step Secure Design Guideline (3SDG). In order to use the enhanced secureUML metamodel for designing a secure system, it needs to follow 3SDG to identify and validate system process. 3SDG is a guideline which is formed by integrating Comprehensive, Lightweight Application Security Process (CLASP) design steps and Sommerville's security guideline which most suitable design guideline. Both guidelines are mainly focuses on designing secure system. By using the enhanced secureUML metamodel with 3SDG in a case study, it ables to show the solution for selected internal threats to improve integrity and Availability. This will help security designer provide protection to the computer which the system runs, application and records from threats. This model and the guideline will able to help to design more persistence secure system to maintain security from internal attacks.

ABSTRAK

Keselamatan adalah dimensi yang paling penting untuk sistem yang melibatkan pemprosesan dan pertukaran maklumat sulit. Oleh itu, ia adalah satu kemestian untuk direka supaya ia mencapai tahap yang tinggi pada keselamatan. Keselamatan bahasa spesifikasi boleh digunakan untuk mewakili spesifikasi keselamatan seperti serangan spesifikasi atau lebih tepat tentang siapa yang boleh melakukan apa dan bila, dan ini boleh dicapai dengan mengekuatkuaskan kawalan masuk. Pendekatan yang sesuai untuk menguatkuaskan kawalan masuk adalah Kawalan Masuk Berasaskan Peranan (RBAC). Hanya metamodel secureUML menggunakan RBAC sebagai mekanisma keselamatan. Walaubagaimana pun, metamodel secureUML tidak menunjukkan sifat-sifat yang menyokong keperluan keselamatan asas yang memberi tumpuan kepada Integriti dan Kebolehsediaan, dan juga pertimbangan keadaan yang membawa kepada kemungkinan serangan yang berbeza. Objektif disertasi ini adalah untuk mencadangkan satu garis panduan reka bentuk sistematik yang selamat dengan meningkatkan metamodel secureUML. Ini adalah untuk meningkatkan prestasi dengan mengintegrasikannya dengan Perlindungan-Tahap Lapisan Bersekuriti yang menyediakan perlindungan bagi aset yang penting dalam pelbagai lapisan untuk menyokong Integriti dan Kebolehsediaan dan untuk mengenal pasti ancaman dalaman yang mungkin berdasarkan senario dengan menggunakan Langkah-demi-Langkah Panduan Rekabentuk Selamat (3SDG). Untuk menggunakan metamodel secureUML yang dipertingkatkan untuk mereka bentuk sistem yang selamat, ia perlu mengikuti 3SDG untuk mengenal pasti dan mengesahkan proses sistem. 3SDG adalah satu garis panduan yang dibentuk dengan mengintegrasikan Komprehensif, Proses Keselamatan Aplikasi Ringan (CLASP) Langkah Rekabentuk dan Garis Panduan Keselamatan oleh Sommerville adalah garis panduan rekabentuk yang paling sesuai. Kedua-dua garis panduan ini terutamanya, memberi tumpuan kepada rekabentuk sistem yang selamat. Dengan menggunakan metamodel secureUML yang dipertingkatkan dengan 3SDG dalam Kajian Kes, dapat menunjukkan penyelesaian bagi ancaman dalaman terpilih untuk peningkatan Integriti dan Kebolehsediaan. Ini akan dapat membantu perekam keselamatan menyediakan perlindungan kepada komputer yang sistem beroperasi, aplikasi dan rekod dari ancaman. Model dan garis panduan ini juga akan dapat membantu rekabentuk sistem untuk mengekalkan sistem yang lebih selamat bagi menyenggara keselamatan daripada serangan dalaman.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGMENT	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	xi
	LIST OF FIGURES	xiii
	LIST OF ABBREVIATIONS	xv
	LIST OF APPENDICES	xvii
1	INTRODUCTION	
1.1	Introduction	1
1.2	Problem Background	3
1.3	Problem Statement	8
1.4	Research Aim	9
1.5	Research Objectives	10
1.6	Research Scope	10
1.7	Significance of Study	11
2	LITERATURE REVIEW	
2.1	Introduction	12
2.2	Overview Of Security	12
	2.2.1 Characteristics of System Security	14

2.3	Overview Of Threats	15
2.3.1	Classification of Threats	16
2.3.2	Internal and External Threats	17
2.4	Software Design	18
2.4.1	Unified Modeling Language	18
2.4.2	Significance of Secure Design	19
2.4.3	Secure Layered Architecture	21
2.5	Secure Software Design	22
2.5.1	Secure Design Languages	23
2.5.2	Security Specification Languages	23
2.5.3	Comprehensive Comparison of Existing Security Specification Languages	27
2.5.4	Compulsory Requirements for a Security Requirements Specification Language	27
2.5.5	Similarity with Software Specification Languages	28
2.5.6	Secure Design Guidelines	28
2.5.6.1	Sommerville's Security Guideline	33
2.5.6.2	The Comprehensive, Lightweight Application Security Process (CLASP)	37
2.6	Security Specification Language for Secure Design	38
2.6.1	Misuse Case	38
2.6.2	SecureUML	40
2.6.2.1	SecureUML Metamodel	41
2.6.2.2	Benefits Of Using SecureUML	42
2.6.2.3	SecureUML – Design Steps	43
2.6.2.4	Access Control	43
2.6.2.5	The Purpose And Fundamentals Of Access Control	44
2.7	Architectural Design Act as Security Classification Model	45
2.7.1	Role-Based Access Control	50
2.8	Security Concern In Software Development Life Cycle (SDLC)	51
2.9	Related Work	55
2.10	Summary	58

3 METHODOLOGY

3.1	Introduction	59
3.2	Research Process Flow Chart	59
3.3	Conceptual Model	63
3.4	Summary	65
4	ANALYSIS ON INTERGRATION OF PROTECTION LEVEL OF SECURE LAYERS INTO SECUREUML	
4.1	Introduction	66
4.2	Integrity And Availability	68
4.3	Affect of Threats towards Integrity and Availability	68
4.3.1	System Security Decision	69
4.3.2	Types of Threats	70
4.3.2.1	Correlation of Threats According CIA	71
4.4	Process of Assimilating Protection-Levels Of Secure Layers Into SecureUML Metamodel	77
4.5	Analyze And Compare Of Protection-Levels Of Secure Layers	79
4.6	Analyze On The Components Of SecureUML Metamodel	81
4.7	The Similarity Between Misuse Cases, SecureUML Secure Layers And Security Policy	82
4.7.1	Mapping Each Protection-Levels Into SecureUML Metamodel Components	84
4.8	Integration of Protection-Levels into SecureUML Metamodel	87
4.8.1	Process of Improving Initial SecureUML Metamodel	88
4.8.2	Stereotypes	90
4.8.2.1	Creation of Access Control Stereotypes	91
4.9	Analysis of Integrated SecureUML Metamodel with Protection-Levels	92
5	EVALUATION ON STEP-BY-STEP SECURE DESIGN GUIDELINE (3SDG)	
5.1	Introduction	94
5.2	Workflow To Produce Step-By-Step Secure Design Guideline (3SDG)	96
5.2.1	Choosing Suitable List Of Guidelines For Secure Design	96
5.2.2	Analyze Clasp Design Steps With Chosen Somerville's Guidelines	99

5.3	Production Of Step-By-Step Secure Design Guideline (3SDG)	101
5.4	Evaluate The Step-By-Step Secure Design Guideline (3SDG) On Case Study	103
5.4.1	Case Study: Meeting Scheduler	103
5.4.2	Application 3SDG On Meeting Scheduler System	107
5.5	Enhance the Integrated SecureUML Metamodel with Protection-Levels using 3SDG	118
5.6	Discussion on the Comparison between Initial Case Study and Proposed Enhanced SecureUML with 3SDG	124
6	CONCLUSION AND FUTURE WORK	
6.1	Introduction	127
6.2	Research Conclusion	127
6.3	Contribution	130
6.3.1	Point Of Body Of Knowledge	130
6.3.2	Practitioners View	131
6.4	Future Work	131
	REFERENCES	132