

Sudan University for Science and Technology
College of Graduated Studies



**Implementation and Evaluation of Systems
Security for Engineering Capability and
Maturity Model**

التقويم والتطبيق لنموذج قياس قابلية ونضج
هندسة الأنظمة الآمنة

**A Masters Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree "Masters in Software Engineering" (M.Sc.)**

Prepared by:

Krunal Shushilkant Mithani

Supervisor:

Dr. Awad Mohammed Awad

2010

ساهم الانتشار الواسع المتزايد لتطبيقات الأعمال الإلكترونية والموبايل في النمو المتطرد للإهتمام بتأمين نظم المعلومات، وعليه أصبح تأمين منتجات وخدمات البرامج يلعب دوراً مؤثراً في صناعة البرامج. فشملت دورة حياة تطوير البرامج متطلبات وآليات التأمين في كل مراحلها، لأنه غير ملائم أن يكون التأمين من الخصائص المضافة لمنتجات البرامج. يهدف هذا البحث لقياس قابلية ونضج بيوتات البرامج السودانية في تطوير وصناعة برامج آمنة وفق إحدى النماذج القياسية واسعة الاستخدام وهو نموذج قياس قابلية ونضج هندسة الأنظمة الآمنة (SSE-CMM). وقد تم تطوير آلية لجمع البيانات بخصوص ممارسات هندسة الأنظمة الآمنة لتلك البيوتات و من ثم تحليل وتقييم النتائج ذات الصلة، والتي تخلص إلى أن ممارسات هندسة الأنظمة الآمنة متباينة جداً بين تلك الشركات، والمفاجئ في الأمر لا توجد شركة استوفت المستوى الأول وفق النموذج القياسي المتبع، مما قد يعكس حقيقة ممارسات التأمين لمنتجات البرمجيات.

Abstract

Increased use of Electronic and Mobile Businesses (E/M-business) as well as their countless associated applications has introduced a growing concern about information system security. Hence security of software products and services plays a major role in software industry. Since software security feature is not appropriate to be added through the addition of sets of features, it must be designed and integrated with the every phase of the software development life cycle.

The aim of this thesis is to measure the capability and maturity of some Sudanese software companies in developing secure software products. In order to achieve above goal, this thesis has used widely accepted standard System Security Engineering Capability Maturity Model (SSE-CMM) as a reference model.

Surveys were conducted in some of the local software companies to gather the data regarding the system security engineering practices being performed. Data collected from the surveys were analyzed and were statistically compared. Results obtained from the analysis indicated that security engineering activities practiced by the companies differ from one to another and none of the companies succeeded in achieving SSE-CMM Level 1, which might reflect the actual security practices for the developed software products.

Acknowledgements

First and foremost, I would like to thank God for his extreme mercy and blessings that lead me to reach this stage.

Special thanks go to Dr. Awad AwadelKarim, my supervisor, for being extremely supportive during the entire process of this research.

Finally warm thanks and gratitude go to my parents, and my close friends for constantly being there for me.

Table of Contents

المستخلص.....	
II	
Abstract.	
III	
Acknowledgements.	
IV	
List of Figures.	VII
List of Tables.	VIII
Chapter 1 Introduction	
1.1 Introduction.....	2
1.2 Problem Definition.....	2
1.3 Research Objectives.....	3
1.4 Research Importance.....	3
1.5 Research Scope.....	4
1.6 Thesis Organization.....	4
Chapter 2 Literature Review	
2 Introduction.....	7
2.1 Background.....	7
2.1.1 Introduction to SSE-CMM Model.....	7
2.1.2 Reasons for developing the model.....	7
2.1.3 SSE-CMM Scope and Application.....	8
2.1.4 Problem that can be solved using SSE-CMM.....	9
2.1.5 Primary benefits of using CMM.....	9
2.1.6 SSE-CMM Project Composition.....	10
2.1.7 SSE-CMM Architecture Description.....	11
2.1.8 Security Engineering Process Areas.....	18
2.1.9 Benefits of using SSE-CMM.....	29
2.2 Related Work.....	30
Chapter 3 Research Methodology	
3 Introduction.....	35
3.1 Phases conducted during Research.....	35
3.2 Standards and Tools used.....	36
Chapter 4 Development and Customization of Questionnaires	
4 Introduction.....	39
4.1 Design of Questionnaires.....	39
4.1.1 Questionnaire Document Design.....	39

4.1.2 Questionnaire Application Design	42
4.2 Assessment Criteria.	45

Chapter 5 Results Presentation, Analysis and Discussions

5 Introduction	47
5.1 Selection Criteria for Companies	47
5.2 Companies Descriptions.	47
5.3 Results Obtained.	48
5.4 Detailed Results.	71
5.5 Rating Profiles of Companies	77
5.5.1 Company A Rating Profile	
77	
5.5.2 Company B Rating Profile	78
5.5.3 Company C Rating Profile	79
5.5.4 General Rating Profile	80
5.6 Results Findings.	81

Chapter 6 Conclusion and Recommendation

6.1 Conclusion.	84
6.2 Recommendations for Future Work	84
6.3 Limitations.	84

References.	85
------------------------------	----

Appendix

Organization Appraisal Questionnaires.	87
--	----

List of Figures

Figure No.	Figure Title	Page No.
2.1	SSE-CMM Project Structure	10
2.2	Relationship between Base Practices and Generic Practices	12
2.3	SSE-CMM Capability Levels	16
4.1	Questionnaire Document Format	41
4.2	Use Case Diagram of Questionnaire Application	42
4.3	Class Diagram of Questionnaire Application	43
4.4	Sequence Diagram of “Select Process Area” Use Case	43
4.5	Sequence Diagram of “Check Status” Use Case	44
4.6	Maturity Level Calculation Algorithm	45
5.1	PA01 Administer Security Controls Results	50
5.2	PA01 Administer Security Controls Maturity Level	50
5.3	PA02 Assess Impacts Results	52
5.4	PA02 Assess Impacts Maturity Level	52
5.5	PA03 Assess Security Risks Results	54
5.6	PA03 Assess Security Risks Maturity Level	54
5.7	PA04 Assess Threats Results	56
5.8	PA04 Assess Threats Maturity Level	56
5.9	PA05 Assess Vulnerability Results	58
5.10	PA05 Assess Vulnerability Maturity Level	58
5.11	PA06 Build Assurance Argument Results	60
5.12	PA06 Build Assurance Argument Maturity Level	60
5.13	PA07 Coordinate Security Results	62
5.14	PA07 Coordinate Security Maturity Level	62
5.15	PA08 Monitor Security Posture Results	64
5.16	PA08 Monitor Security Posture Maturity Level	64
5.17	PA09 Provide Security Inputs Results	66
5.18	PA09 Provide Security Inputs Maturity Level	66
5.19	PA10 Specify Security Needs Results	68
5.20	PA10 Specify Security Needs Maturity Level	68
5.21	PA11 Verify and Validate Security Results	70
5.22	PA11 Verify and Validate Security Maturity Level	70
5.23	Detailed Results of Company A	72
5.24	Detailed Results of Company B	74
5.25	Detailed Results of Company C	76
5.26	Rating Profile of Company A	77
5.27	Rating Profile of Company B	78
5.28	Rating Profile of Company C	79
5.29	General Rating Profile	80

List of Tables

Table No.	Table Title	Page No.
1.1	Thesis Organization	4
2.1	List of Maturity Models for Security	31
2.2	Comparison of the SSE-CMM to the Related Efforts	32
4.1	Assessment Criteria	45
5.1	Companies Descriptions	47