DEVELOPMENT OF SECUREMET : A TOOL FOR ALIGNING SECURITY METRICS AND ORGANIZATIONS SECURITY OBJECTIVES

A project submitted to Dean of Awang Had Salleh Graduate School of arts and Science in partial Fulfillment of the requirement for the degree Master of Science (Information Technology) Universiti Utara Malaysia

By
Noraini binti Mohd Noor
DEVELOPMENT OF SECUREMET: A TOOL FOR ALIGNING SECURITY METRICS AND ORGANIZATIONS SECURITY OBJECTIVES

NORAINI BINTI MOHD NOOR

UNIVERSITI UTARA MALAYSIA
2011
PERMISSION TO USE

In presenting this project in partial fulfillment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this project in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor or, in their absence by the Dean of Awang Had Salleh Graduate School of Arts and Sciences. It is understood that any copying or publication or use of this project or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my project.

Requests for permission to copy or to make other use of materials in this project, in whole or in part, should be addressed to

Dean of Awang Had Salleh
Graduate School of Arts and Sciences College of
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman
Malaysia
ABSTRACT (BAHASA MALAYSIA)

ABSTRACT (ENGLISH)

The purpose of this project is to develop a tool henceforth called SecureMet to help an organization to determine the security metrics aligned with its security objectives based on the organization’s capabilities. The majority of organizations face a common problem in determining their security metrics aligned with their security objectives. SecureMet will be able to assist the organization in choosing the suitable security metrics and helping it to enhance its capabilities to achieve its security objectives. The tool is developed based on the Quality Function Development (QFD) approach, while existing frameworks such as the SSE-CMM and COBIT are used as guides in the determination and choice of the security capabilities and security objectives. The methodology employed for this project is based on the Rapid Application Development (RAD) model and is divided into four parts, namely, the requirement analysis phase, the design phase, the development phase and the verification phase.
ACKNOWLEDGEMENT

Praise and gratitude be given to Allah the Almighty for putting forward me such a great strength, patience, courage, and ability to complete this project.

My gratefulness to my supportive and helpful supervisor, Prof. Nazib bin Nordin for assisting and guiding me in the completion of this project. With all truthfulness, without him, the project would not have been a complete one. He has always been my source of motivation and guidance. I am truly grateful for his continual support and cooperation in assisting me all the way through the semester.

I would like to present my thanks to my father, my mother, my husband and all my family who has always been there for me. Finally, I would like to express my appreciations to all my friends, colleagues, Examinations Unit staff, and everyone who has helped me in this journey.
TABLE OF CONTENTS

PERMISSION TO USE ........................................... I
ABSTRACT (BAHASA MALAYSIA) ................................ II
ABSTRACT (ENGLISH) ........................................... III
ACKNOWLEDGMENTS ........................................... IV
TABLE OF CONTENTS .......................................... V
LIST OF FIGURES ............................................. IX
LIST OF ABBREVIATIONS ..................................... XI

CHAPTER ONE : INTRODUCTION

1.1 Background .................................................. 1
1.2 Problem Statement .......................................... 5
1.3 Project Questions ........................................... 6
1.4 Project Objectives .......................................... 6
1.5 Scope of Project ............................................ 7
1.6 Significance of the Study ................................. 7
1.7 Organization of the Report ............................... 8
CHAPTER TWO : LITERATURE REVIEW

2.1 Security Metrics .................................................................10
2.2 Quality Function Deployment (QFD) .................................15
2.3 Security Objectives .......................................................... 20
   2.3.1 Control Objectives for Information and
         Related Technology (C0BIT) .................................21
2.4 Security Capabilities ....................................................... 26
   2.4.1 System Security Engineering Capability
         Maturity Model (SSE-CMM) ................................. 27
2.5 Summary ................................................................. 32

CHAPTER THREE : PROJECT METHODOLOGY

3.1 Introduction ........................................................................33
   3.1.1 Requirement Analysis Phase .................................34
   3.1.2 Design Phase ..........................................................36
   3.1.3 Construction Phase ..................................................37
   3.1.4 Verification Phase ....................................................39
3.2 Tool Development ............................................................40
3.3 Project Planning ..............................................................40
3.4 Summary .................................................................40
CHAPTER FOUR : METHOD FOR DEFINING SECURITY METRICS : SECUREMET

4.1 Introduction .........................................................................................................................41

4.2 Method Description .............................................................................................................42
  4.2.1 Preparation ......................................................................................................................45
  4.2.2 Performing the Alignment ..............................................................................................47
  4.2.3 Step 10 – Analysis ........................................................................................................49

4.3 Tool Development .............................................................................................................50
  4.3.1 Tool Support ................................................................................................................50
  4.3.2 Tool Screen ..................................................................................................................50

4.4 Summary .............................................................................................................................55

CHAPTER FIVE : FINDING AND DATA ANALYSIS

5.1 Data Finding .......................................................................................................................56
  5.1.1 Preparation ...................................................................................................................56
  5.1.2 Perform the Alignment .................................................................................................64

5.2 Data Analysis .....................................................................................................................67

5.3 Summary .............................................................................................................................69
CHAPTER SIX : CONCLUSION

6.1 Project Contribution ..........................................................70
6.2 Limitation and Future Work ............................................ 71
6.3 Conclusion ........................................................................ 71
6.4 Summary ........................................................................ 73

REFERENCES ........................................................................... 74

APPENDICES ............................................................................ 82

Appendix A: Description of Security Capabilities ................... 82
Appendix B: Security Objectives against Capabilities page ...... 84
Appendix C: Security Capabilities against Security Metrics page .. 85
Appendix D: Graph page .......................................................... 86
Appendix E: Questionnaire .................................................... 87
LIST OF FIGURES

Figure 2.1: Management Framework (Versmissen, 2007) .................14
Figure 2.2: Method of Security Metrics (Versmissen, 2007) ...............15
Figure 2.3: House of Quality matrix (Becker, 2000) .........................18
Figure 2.4: COBIT IT Processes defined within the Four Domains ..........24
Figure 2.5: Control Objective Summary Table
(IT Governance Institute, 2007) .............................................26
Figure 2.6: SSCAM structure (Simpton, J.J and Endicott, B , 2010) .....30
Figure 2.7: The Process of Mapping SSE-CMM into Patient-Centered Healthcare Domain (Huang, 2008) .........................31
Figure 3.1: The RAD Model (Whitten, 2004) ................................34
Figure 3.2: Requirement Analysis Phase ....................................35
Figure 3.3: Design Phase ....................................................37
Figure 3.4: Construction Phase ............................................. 38
Figure 3.5: Verification Phase ............................................. 39
Figure 3.6: Gantt Chart ....................................................40
Figure 4.1: Relationship between security objectives, capabilities and metrics (Fruehwirth, C. et al., 2010) .......... 42
Figure 4.2: The SecureMet Architecture .................................... 43
Figure 4.3: Alignment Method (Fruehwirth, C. et al., 2010) ............... 44
Figure 4.4: SecureMet Login ............................................... 51
Figure 4.5: List of Security Objectives and Standard Deviation Calculation Page ......................................................... 51
Figure 4.6: List of Security Capabilities and Standard Deviation Calculation Page ..................................................... 52

Figure 4.7: Security Objectives against Capabilities Page ...................... 53

Figure 4.8: Security Capabilities against Security Metrics Page ........... 54

Figure 4.9: Graph Showing Security metrics and its alignment Scores ... 55

Figure 5.1: List of Security Objectives .............................................. 57

Figure 5.2: Top 10 Security Objectives ............................................. 58

Figure 5.3: Weight of Security Objectives ........................................... 59

Figure 5.4: List of Security Capabilities ............................................... 60

Figure 5.5: List of 10 Security Capabilities .......................................... 61

Figure 5.6: Weight of Security Capabilities ....................................... 61

Figure 5.7: Matrix 1 .......................................................................... 62

Figure 5.8: Security Metrics ................................................................. 63

Figure 5.9: Matrix 2 ........................................................................... 64

Figure 5.10: Matrix 1 (with values input 3(high), 2(Medium),

1(low), and 0(none)) ........................................................................ 65

Figure 5.11: Matrix 2 (with values input 3(high), 2(Medium),

1(low), and 0(none)) ........................................................................ 67

Figure 5.12: Graph (Security Metrics to Alignment Scores/

Cumulated impact) ......................................................................... 68

Figure 5.13: sequence of Alignment Scores/Cumulated Impact ........... 69
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>COBIT</td>
<td>Control Objectives for Information and Related Technology</td>
</tr>
<tr>
<td>CVSS</td>
<td>Common Vulnerability Scoring System</td>
</tr>
<tr>
<td>I3P</td>
<td>Institute for Information Infrastructure Protection</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>KGI</td>
<td>Key Goal Index</td>
</tr>
<tr>
<td>KPI</td>
<td>Key Performance Index</td>
</tr>
<tr>
<td>POLIMAS</td>
<td>Politeknik Sultan Abdul Halim Mu'adzam Shah</td>
</tr>
<tr>
<td>QFD</td>
<td>Quality Function Deployment</td>
</tr>
<tr>
<td>RAD</td>
<td>Rapid Application Development</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SECMET</td>
<td>Security Metrics</td>
</tr>
<tr>
<td>SPI</td>
<td>Software Process Improvement</td>
</tr>
<tr>
<td>SSCAM</td>
<td>System Security Capability Assessment Model Development and Application</td>
</tr>
<tr>
<td>SSE-CMM</td>
<td>System Security Engineering Capability Maturity Model</td>
</tr>
</tbody>
</table>
CHAPTER ONE

INTRODUCTION

This chapter discusses on the background of the study by quoting some facts from journals. It is followed by the problem statement, the project questions, the objectives of the study, and the significance of the study. The scope and the limitations of the study are also included in this chapter.

1.1 Background

In today’s era, most business processes are closely tied to information technology (IT). As a result of its dependence on IT, the need for security in the IT systems is highly desirable. The use of IT applications in many fields has increased tremendously over the years and there seems to be no let up in its importance. Currently, the internet is not only a source for information but has fast become a medium for many kinds of business transactions. Organizations today need to hook up onto the global network and breaking national geographical barriers, to communicate and deal with ever increasing number of customers, suppliers, clients, business partners and, also their own employees. However this IT connection has its ever present and constant threat from malicious hacking activities. The threat from theft of confidential information from an organization is often the case but a more harmful threat may involve a system failure. Due to increase in internet
The contents of the thesis is for internal user only
REFERENCES


Liu, X.F., Sun, Y., Kane, G., Kyoya, Y., & Noguchi, K. QFD application in software process management and improvement based on CMM.


