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)

Tujuan projek ini adalah membangun satu alat iaitu SecureMet untuk membantu organisasi dalam menentukan metrik keselamatan yang sejajar dengan objektif keselamatan berdasarkan kepada keupayaan organisasi tersebut. Kebanyakan organisasi menghadapi masalah dalam penentuan metric keselamatan sejajar dengan objektif keselamatan organisasi. SecureMet ini dapat menyumbang organisasi dalam pemilihan metrik keselamatan yang paling sesuai dan juga dapat meningkatkan keupayaan untuk mencapai objektif keselamatan organisasi. Alat yang dibangunkan ini adalah mengikut pendekatan daripada *Quality Function Development* (QFD). Manakala rangkakerja yang sedia ada seperti SSE-CMM dan COBIT digunakan sebagai panduan dalam pemilihan keupayaan keselamatan dan objektif keselamatan. Methodologi yang digunakan untuk projek ini adalah bedasarkan kepada model *Rapid Application Develoment* (RAD) dan dibahagikan kepada empat fasa iaitu fasa analisis, fasa reka bentuk, fasa pembangunan, dan fasa pengesahan.

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 Develoment (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 him 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

CHAPTER ONE : INTRODUCTION

CHAPTER TWO : LITERATURE REVIEW

CHAPTER THREE : PROJECT METHODOLOGY

CHAPTER FOUR : METHOD FOR DEFINING SECURITY METRICS : SECUREMET

CHAPTER FIVE : FINDING AND DATA ANALYSIS

CHAPTER SIX : CONCLUSION

LIST OF FIGURES

LIST OF ABBREVIATIONS

COBIT	Control Objectives for Information and Related Technology
CVSS	Common Vulnerability Scoring System
I3P	Institute for Information Infrastructure Protection
IT	Information Technology
KGI	Key Goal Index
KPI	Key Performance Index
POLIMAS	Politeknik Sultan Abdul Halim Mu'adzam Shah
QFD	Quality Function Deployment
RAD	Rapid Application Develoment
SCADA	Supervisory Control and Data Acquisition
SECMET	Security Metrics
SPI	Software Process Improvement
SSCAM	System Security Capability Assessment Model Development and Application
SSE-CMM	System Security Engineering Capability Maturity Model

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

Akao, Y. (1990). Quality Function Deployment, Productivity Press, Cambridge MA

Anderson, O. (1990). The use of Software Engineering Data in Support of Project Management. *Software Engineering Journal, 5(6),* 350-356.

Basili, V., Caldiera, G., & Rombach, D. (1994). The Goal Question Metric Approach in Encyclopedia of Software Engineering (pp. 528-532): John Wiley and Sons Inc.

Becker, E.L., et al (2008). Strategic Alignment of Software Process Improvement Programs Using QFD. ACM

Bellovin, S. M. (2006). On The Brittleness Of Software And The Infeasibility Of Security Metrics. *IEEE Security & Privacy, 4(4):96*, July–August.

Brotby, W. K. (2009). Information security management metrics: a definitive guide to effective security monitoring and measurement. Boca Raton, FL: Taylor & Francis Group, LLC.

Cheng, X. R. (2007). Fuzzy Security Assessment of Entropy-Weight Coefficient Method Applied in Electric Power Information Systems.Power Engineering Conference, IPEC 2007.

Croteau, A., And Bergeron, F. (2001). An information technology trilogy: business strategy, technological deployment and organizational performance. *Journal of Strategic Information Systems 10*, 77-99.

Curtis, B., Hefley, W.E., And Miller, S.A. (2001). People Capability Maturity Model: Version 2.0. Retrieved October 3, 2011, from http://www.sei. cmu.edu/pub/documents/ 01.reports/pdf/01mm001.pdf.

Dennis, A., Wixom, B.H., & Tegarden, D. (2005). System Analysis And Design With UML Version 2.0. Danvers: Wiley.

Fenton, N. E., & Neil, M. (1999). Software Metrics: Successes, Failures and New Directions. *The Journal of Systems and Software, 47*, 149-157.

Fruehwirth, C. et al (2010). Addressing Misalignment Between Information Security Metrics and Business-Driven Security Objectives. MetriSec, Italy.

Fulton, & Bradley. (2001). The Weakest Link: The Human Factor. 29 August 2001. Retrieved 6 October 2011, from URL: http://www.sans. org/rr/encryption/human.php.

Gheorghe, G (2009).A Governance and Compliance Maturity Model WISG'09, November 13, 2009, Chicago, Illinois, USA. ACM

Hauser, J.R., & Clausing, D. (1996). The House Of Quality. *IEEE Engineering Management Review 24*, 24–32.

Herzwurm, G. et al. (2003). QFD for customer – Focused Requirement Engineering. *IEEE International Requirements Engineering Conference*

Honeywell. 2003. Alarm Performance Benchmarks– *User's Guide.* Honeywell International, Morristown, New Jersey.

Huang, (2008). Developing a SSE-CMM-based Security Risk Assessment Process for Patient-Centered Healthcare Systems. Germany.

Ince, D., Sharp, H., & Woodman, M. (1993). Introduction to Software Project Management and Quality Assurance London: McGraw Hill Book Company.

IT Governance Institute, *COBIT Executive Summary, 3rd Edition*, Released by COBIT Steering Committee, pp. 3, July 2000.

Jaquith, A. (2007). Security metrics: replacing fear, uncertainty, and doubt. Upper. Saddle River, NJ: Pearson Education, Inc.

Jensen, F. (2001).Bayesian Networks and Decision Graphs. Springer-Verlag, New York, USA.

Kongsuwan, P., Shin, S., & Choi, M. (2008). Managing Quality Level for Developing Information Security System Adopting QFD. *Software Engineering, Artificial Intelligence, Networking, and Parallel/ Distributed Computing, 2008. SNPD'08. Ninth ACIS International Conference on*, 19–24.

Lee, J. et al (2003). ACC-based Security Engineering Process Evaluation Model. *Proceedings of the 27th Annual International Computer Software and Applications Conference (COMPSAC'03)*

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

Liu, X. F., et al. (2005). QFD Application in Software Process Management and Improvement, St Louis, Missouri, *Proceedings of the third workshop on Software quality*, 6USA.Copyright ACM.

Mathew, N., & Brian, C. (2007). A Metrics Generation Model for Measuring the Control Objectives of Information Systems Audit. *Proceedings of the 40th Hawaii International Conference on System Sciences*.

Mead, N.R. & INST, C.U.P.P.S.E. (2006) Experiences in Eliciting Security Requirements.

Mellado, D. et al. (2010). A Comparison of Software Design Security Metrics. *ECSA 2010, August 23–26,* Copenhagen, Denmark*. ACM*

Moller, K. H., & Paulish, D. J. (1993). Software Metrics: A Practitioner's Guide to Improved Product Development London Chapman & Hall Computing.

Morimoto, S. (2009). Application of COBIT to Security Management in Information Systems Development. *International Conference on Frontier of Computer Science and Technology.*

Nunes, F.J. (2010). Security Engineering Approach to Support Software Security. *IEEE 6th World Congress on Services.* Brazil.

Oza, N., Biffl, S., Fruthwirth, C., Selioukova, Y., & Sarapisto, R. (2008). Reducing the Risk of Misalignment between Software Process Improvement Initiatives and Stakeholder Values. *Industrial Proceedings of EuroSPI*, 6–9.

Patriciu, V.T (2006). Security Metrics For Enterprise Information Systems. *Applied Quantitative methods, Vol 1*. New York.

Paulk, M.C. (2001). A history of the Capability Maturity Model for software. Retrieved October 6, 2011. from http://www.sei.cmu.edu/cmm/slides/cmm-history.pdf

Paulk, et al. (1993). Capability Maturity Model for Software, Version 1.1, *Software Engineering Institute*, CMU/SEI-93-TR-24, February.

Pfahler, M., & Jens, H. (2008). Clinical Information System - A Case Study.ACM. Canada.

Phillips, M. (2003). Using a Capability Maturity Model to Derive Security Requirements. SANS Institute

Proctor, P.E., & Byrnes, F. C., (2002). Secured Enterprise, The: Protecting Your Information Assets. Prentice HallJensen, F.

Rathbun, D. (2009). Gathering Security Metrics and Reaping the Rewards Sans Institute.

Ridley, G. et al. (2004). COBIT and its Utilization: A framework from the literature. Proceedings of the 37th Hawaii *International Conference on System Sciences*

Sabherwal, R., & Chan, Y.E. (2001). Alignment between business and IS strategies: a study of prospectors, analyzers, and defenders. *Information Systems Research* 12, 11-33.

Schneier, B. (2001). Managed security monitoring: network security for the 21st century. *Computers and Security 20(6*): 13.

Seddigh, N., et al (2004). Current Trends and Advances in Information Assurance Metrics. *Proc. of the 2nd Ann. Conf. Privacy, Security and Trust* (PST 2004), Fredericton, NB, Oct.

Simpson, J.J., & Endicott, B. (2010). System Security Capability Assessment Model Development and Application. Retrieved October 3, 2011, from http://www.eskimo.com/jjssbw/staticfiles/INCOSE10SSCAMSlides.pdf

Sommerville. I. (2001). Software Engineering (61h ed.). Harlow, England: Addison Wesley.

Stefani et.al. (2009). Meta-metric Evaluation of E-Commerce-related Metrics. Retrieved October 5 2011, from http://quality.eap.gr/Meta-metric Evaluationof20ECommerce.pdf

Stoddard, M. et al., (2005). Proces control System Security Metric. Trustees Dartmouth.United State.

Syed Jamal Hussain & Muhammad Sibghatullah Siddiqui. (2005). Quantified Model of COBIT for Corporate IT Governance. *First international conference.ICICT*

VanZyl, A.J. (2001)**.** The process innovation imperative and the software producing organization. Johannesburg: University of the Witwatersrand. (PhD thesis).

Vaughn, R., Henning, R. & Siraj, A. (2003). Information Assurance Measures and Metrics: State of Practice and Proposed Taxonomy. *Proc. of 36th Hawaii Int. Conf. on System Sciences HICSS 03.*

Verma, et al (1996). Analyzing a Quality Function Deployment (QFD) Matrix: An Expert System Based Approach to Identify Inconsistencies and Opportunities.

Vermissen, P. (2007). Security Metrics. Retrieved September 29, 2011, From http;//www.isaca.be/ content/Peter_Versmissen.pdf

Whitten, J. L. Betley, L.D., & Diltman, D.C. (2004). Systems Analysis and Design Methods. 6th edition. Boston: McGraw-Hill Education.