DEVELOPMENT OF METAMODEL FOR INFORMATION SECURITY RISK MANAGEMENT

MOHAMMED SALEM MOHAMMED BA MUQABEL

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

Faculty of Computing
Universiti Teknologi Malaysia

JUNE 2013

"Dedicated to my beloved family without their understanding, supports, and most of all love, the completion of this work would not have been possible."

ACKNOWLEDGEMENT

I would like to express my gratitude to Allah for providing me the blessing to complete this work. Hence, I am deeply grateful to my supportive and helpful supervisor **Dr Siti Hajar Binti Othman** for assisting and guiding me in the completion of this project. With all truthfulness, without Allah then her support and motivate, this project would not have been a complete. Dr Siti Hajar Binti Othman has always been my source of motivation and guidance. For that, I am truly grateful for her continual support and cooperation in assisting me all the way through my master.

To my family, no words can describe my gratefulness for always being there despite of the distance. They have showered me with love and compassion and enrich my life like no other. They are the source of comfort and kept me focus the priorities in life and therefore, this work is dedicated to them.

My thanks also extend to my friends, for their enlightening companionship and encouragement of trudging through all the moments from down to up the hill in the run to complete Master Project. I would not have done it without the help and motivation from all of them.

ABSTRACT

Nowadays, information technology and information system have been used widely in many fields such as in business, education, marketing, transportation, medical and many other fields. In information technology and system field, a security aspect plays a vital role and thus become a challenging issue. Thus security should be ready installed and resistance to various numbers of potential attacks. In Information Security and Information Technology, it is important to decide what countermeasures that could potentially harm the organization from achieving their business objectives. Reducing risk to an acceptable level is among the main target of the risk management process. On other hand, the main reasons to fail in Information Security Risk Management (ISRM) is the complexity and inflexibility of the existing models. Domain modulars usually spend a lot of times to understand the nature of the domain which they desire to model. Even though there are many existing ISRM models appears, but to find a suit model which could provide a straight guideline to the ISRM users based on their own problems are limited. To solve this issue, this project follows seven steps to create a generic metamodel which can describe the semantics of ISRM models and its solutions through one unified model. Then validates ISRM by three validation techniques; Frequency-based Selection, Face validity and Tracing technique. Through the metamodel various risk management problems faced by different levels of ISRM users can be solved based on the problem attributes such as, risk determination specific to a firewall vulnerability problems, risk assessment for an information security project management. Directly, this can help many users/newcomers to this domain to easy understand the concepts required for their own information security risk problem.

ABSTRAK

Pada masa kini, teknologi maklumat dan sistem maklumat yang telah digunakan secara meluas dalam pelbagai bidang seperti perniagaan, pendidikan, pemasaran, pengangkutan, perubatan dan pelbagai bidang lain. Dalam teknologi dan sistem maklumat bidang, aspek keselamatan memainkan peranan yang penting dan dengan itu menjadi satu isu yang mencabar. Oleh itu, keselamatan harus dipasang siap dan penentangan terhadap pelbagai nombor serangan yang berpotensi. Dalam Keselamatan dan Maklumat Teknologi Maklumat, adalah penting untuk menentukan apa langkah-langkah tindakan yang berpotensi boleh merosakkan organisasi daripada mencapai objektif perniagaan mereka. Mengurangkan risiko kepada tahap yang boleh diterima adalah antara sasaran utama proses pengurusan risiko. Pada tangan yang lain, sebab-sebab utama untuk gagal dalam Maklumat Pengurusan Risiko Keselamatan (ISRM) adalah kompleks dan tidak fleksibel daripada model yang sedia ada. Modulars Domain biasanya menghabiskan banyak masa untuk memahami sifat domain yang mereka inginkan untuk model. Walaupun terdapat banyak model yang sedia ada ISRM muncul, tetapi untuk mencari model yang sesuai yang boleh memberikan satu garis panduan lurus kepada pengguna ISRM berdasarkan masalah mereka sendiri adalah terhad. Untuk menyelesaikan isu ini, projek ini mengikuti tujuh langkah untuk mewujudkan metamodel generik yang boleh menggambarkan semantik model ISRM dan penyelesaian melalui satu model bersatu. Kemudian mengesahkan ISRM oleh tiga teknik pengesahan; Pemilihan berasaskan Frekuensi, kesahan muka dan menilik teknik. Melalui metamodel pelbagai masalah pengurusan risiko yang dihadapi oleh tahap yang berbeza dari pengguna ISRM boleh diselesaikan berdasarkan masalah ciri-ciri seperti, penentuan risiko khusus kepada masalah kelemahan firewall, penilaian risiko untuk pengurusan projek keselamatan maklumat. Secara langsung, ini boleh membantu ramai pengguna / pendatang baru kepada domain ini untuk mudah memahami konsep yang diperlukan untuk masalah risiko keselamatan maklumat mereka sendiri.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDIXES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Nowadays, information technology and information system have been used widely in many fields such as in business, education, marketing, transportation, medical and many other fields. In information technology and system field, a security aspect plays a vital role and thus become a challenging issue. Security is required in this field as a ready-installed resistance to various numbers of potential attacks. This pose a great challenge in ensuring the success of security embedded in the information technology and system field. Risk management is an ongoing and iterative process. In information technology and information security field, risk management can be defined as the process of identifying vulnerabilities and threats to the information resources used by an organization. To decide what countermeasures that could potentially harm the organization from achieving their business objectives is important. Reducing risk to an acceptable level is among the main target of the risk management process.

The necessary of security technologies and technical programs has been recognized on a large scale therefore receiving a continuous attention (for example, new encryption algorithms, public key infrastructure, etc.). Return on Security Investment (ROSI) issues, related to the costs spent on security technologies compared with their benefits. Nevertheless, to protect an organization's business

firstly need to identify and evaluate the relationship between the assets and their security. The essential problem to align the information technology assets and security is through a Risk Management (RM) process. Therefore, to handle the risk of an unexpected events and threats happen to many information security assets and personnel, it is believed that a metamodel could offer its benefit. The organization of the knowledge complexity of this domain can be managed through the artifact called the Information Security Risk Management (ISRM) metamodel. ISRM is a security method that can manage and reduce threats and vulnerabilities and also can mitigate security risks (Xuan, Wuwong et al. 2010). Over time, organizations tend to relax their security posture. To combat a relaxation of security, organization should apply a model to perform security risk management.

In the first chapter, the problem background of this research is explained. This is then continued with a discussion on this research's problem statement. Next, it is followed by a discussion on research question, research objectives, research scopes and a summary of this project structure.

1.2 Problem Background

The reason of failing to prevent disasters and threats on the subsequent management are rarely caused by a single factor. They are often a result of the accumulation of a complex series of events and often accompanied by changes in the external environment factors (Aini, Fakhrul-Razi et al., 2005). It is a common wisdom that there are no two risks exactly having the same impact, each one has its own impact, and that every risk requires its own management process. For example, risk mitigation is an ISRM action that is applicable in many risk situations. Whenever organization faces a problem of risk, usually remembers previous accident scenario involving with same key features with one at hand and apply the solution that worked previously. By matching previously effective actions with the current situation, an appropriate course of action is recalled and put into effect promptly (Paton and Jackson, 2002). Therefore, this research aims to use a generic

representational layer (a metamodel) to give a unified view of common concepts and actions that apply in several of information security risk management.

Complexity and inflexibility of the model for the domain user is an essential reason to fail in many of ISRM. Domain modulars usually spend a lot of times to understand the nature of the domain which they desire to model. Generally, most of them use a general purpose language such as Unified Modeling Language UML in modeling their domain application models. However, when the created models do not perfectly fit their needs. Therefore, a more specific domain modeling language such as ISRM is believed that it can offer a better alternative approach to the problem.

The problem when designing a new model of the domain is the issue of identification of the domain concepts and ambiguity of the concept terminologies. This will be a big problem especially to the newcomers of the domain (in this case, the newcomer is any person who new to the ISRM domain). As with any domain, the power of its domain-specific language is directly tied to the abstraction level of the domain concepts. Thus, the more semantic meaning attached to domain-concepts, the less time the modeler spends specifying the domain models (Sprinkle, 2003). The meaning and definition of specific concept terminologies and their relationships are discipline specific and may differ from one observer to the other one (Gharehdaghli, 2003), so domain concepts can have multiple descriptions. The field of ISRM requires a flexible structure to allow it offering a facility to store and retrieve not only observed and measured data, but also interpretative and inferred information of its domain. Thus through the creation of Information Security Risk Management Metamodel (ISRMM) library the ambiguity problem of ISRM terminologies could be solved.

There are a lot of models are available in for the information security analysis and end user from various fields; it might look as an advantage for them. However, this statement might be true only if the user requirements are the same and well defined. But not, in the wide area such a security risk management that contains

many a huge number of different aspect and terminologies. In order to simplify this activity, the proposed ISRMM is believed can describes all contained ISRM model concepts and the way they are arranged, related and constrained.

These has motivated the researcher in aiming to provide all security risk management users especially the ISRM model developers with a complete set of reference model through the development of ISRMM. The metamodel can provide a wide range of capability encompassing serving to different kinds of security risk in Information Security such as, risk in network or cloud computing, risk in internal or external InfoSec project management, risk in access control process. With various level of ISRM users such as, security manager, information security officers, network technical personnel, IT managers in business, hospital, university and etc.

1.3 Problem Statement

Normally, when people face a problem, they approach facilitates recalling prior incident scenarios that share key features with the one at hand and apply the solution that worked previously. Knowledge of ISRM is huge and scattered everywhere. It is believed that many problems faced by various information security users actually have their own successful solutions. However, because of the solutions are scattered in different places and also takes time to find it, therefore, it is difficult for the current users ,who may be facing the same problem, to reuse the solution based on their own security risk management problem. In information security field, many organizations either in both public and private sectors suffer with the complexity and inflexibility of the information security risk framework and models. Even though there are many existing ISRM models that appears, but to find a suiting model which could provide a straight guideline to the ISRM users based on their own problems are limited. To solve this issue, this project creates a metamodel which can describe the semantics of ISRM models and its solutions through one unified model. For metamodel, the concepts created in the artifact will come together with the repository (domain solution) of the concept. It is believed, through the

metamodel various risk management problems faced by different levels of ISRM users can be solved based on the problem attributes such as risk determination specific to a firewall vulnerability problems, risk assessment for information security project management. Directly, this can help many users/newcomers to this domain to easily understand the concepts required for their own information security risk problem.

1.4 Research Questions

In order to address the issues highlighted in the previous section, there are two research questions that need to be tackled:

1. How to create a generic ISRM metamodel through the observation against existing domain model?
2. How the proposed ISRM metamodel can provide such a modeling guidelines for various ISRM users in solving their own risk problem?

1.5 Objective of Project

This research has three objectives:

i. To study and analyze how a metamodelling approach could capable to support the complexity of knowledge in the ISRM domain thorough investigation to various existing ISRM models from different sources.

ii. To develop the ISRM Metamodel (a specific modeling language for the ISRM domain) by using the 7-Steps of a metamodel development.

iii. To validate the proposed ISRM metamodel by using the metamodel validation techniques.

1.6 Scope of Project

The scope that identifies the boundaries of the project listed below:

i. The research will focus on the creation of a metamodel in level M2 (the representation of ISRM metamodel) by using the Four-layer Meta Object Facility (MOF) metamodelling framework. The creation will use a set of 10 existing ISRM models.
ii. For the purpose of metamodel validation, the proposed metamodel will use three technique of metamodel validation known as the '*Frequency based Selection', 'Face Validity', and 'Tracing'*. For '*Frequency based Selection'* a set of 3 models (Set V) will be used.
iii. For the purpose of showing the applicable of the metamodel in real world ISRM domain, an instantiation of models from the ISRM metamodel will be presented by using one ISRM case study problem.

1.7 Project Structure

This project is structured into six chapters. To facilitate access to the project, a brief description of the contents of each chapter. Chapter 1: Gives an introduction to the research and guides the reader through a brief description of the research area (problem background, problem statement, research objectives and research scopes). Chapter 2: Provides a review result on the relevant published research work. It also includes the processes and techniques used to create the ISRM metamodel. Chapter 3: Describes a research methodology conducted for this project, where a design science research methodology is used. In here, this project justifies the use of methodology and describes the four phases of the research used in this project: ISRMM problems identification, ISRM metamodel creation and ISRM validation. Chapter 4: Performs the eight steps ISRMM creation process and presents the initial result of the ISRM Metamodel. For this purpose, a set of 10 existing ISRM Models are used.

Chapter 5: Validates the initial version of ISRMM (version 1.0) by applying three validation techniques, Frequency-based Selection, Face Validity and Tracing technique. Chapter 6: Summarizes the research findings, draws conclusions, and outlines future works and possibilities for extending this research.

REFERENCES

Aini, M. S., et al. (2005). "Analysis Of Royal Inquiry Report On The Collapse Of A Building In Kuala Lumpur: Implications For Developing Countries." Disaster Prevention and Management **14**(1): 55-79.

Alhir (2003) Understanding the Model Driven Architecture (MDA).

Andreasen, M., et al. (2002). Design Typology and Design Organisation.

Author (2012). Characteristics of Information Security.

Beers, W. (2005). Kriging Metamodelling For Simulation, Tilburg University. PhD Thesis.

Belle, V. (2004). Framework for Evaluation of Enterprise Model. Cape Town, University of Cape Town. PhD

Beydoun, G., et al. (2009). "FAML: A Generic Metamodel for MAS Development." IEEE Transactions on Software Engineering **35**(6): 841-863.

Bonnette, C. A. (2012) Assessing Threats To Information Security In Financial Institutions

Cook, S. (2004). "Domain-Specific Modeling and Model Driven Architecture." MDA

Cross, N. (2007). Editorial: Forty years of design research. D. Studies.

Garcia, P. B. (2007). A Metamodel To Annotate Knowledge Based Engineering Codes As Enterprise Knowledge Resources, Cranfield University. **PhD** 489.

Gargantini, A., et al. (2009). "A semantic framework for metamodel-based languages." Automated Software Engineering **16**(3): 415-454.

Geotgetown_University (2013). Georgetown University's Risk Management Process

Gharehdaghli, A. (2003). Design of a Generic Metamodel for Fieldwork Data Management. International Institute For Geo=Information, Science and Earth Observation Enschede, Netherlands. Master of Science in Geoinformatics.

Goeken, M. and S. Alter (2009). Towards Conceptual Metamodeling of IT Governance Frameworks Approach - Use - Benefits. Hawaii International Conference on System Sciences.

Herold, R. (2002). "What is the Difference Between Security and Privacy." CSI.

Hevener, A., et al. (2004). Design Science in Information Systems Research. MIS Quarterly.

Hevner, A. and S. Chatterjee (2010). "Design Science Research in Information Systems." Springer US.

Hevner, A., et al. (2004). Design Science in Information Systems Research. MIS Quarterly.

Institute, S. (2003). Global Information Assurance Certification Paper. Information Risk Assessment.

ISO/IEC:27001, I. O. f. S. (2005). ISO/IEC 27001. Information technology - Security techniques - Information security management systems Requirements. Geneva.

ISO/IEC:27005, I. O. f. S. (2008). ISO/IEC 27005. Information technology - Security techniques - Information security risk management. Geneva.

ISO/IEC_Guide73, I. O. f. S. (2002). ISO/IEC Guide 73. . Risk management - Vocabulary - Guidelines for use in standards. Geneva.

ISO:3100, I. O. f. S. A. N. (2009). AS/NZS ISO 3100. Risk management - Principles and guidelines. Australia, Standards Australia/ Standards New Zealand.

Jalali, V. and M. Matash Borujerdi (2011). "Information retrieval with concept-based pseudo-relevance feedback in MEDLINE." Knowledge and Information Systems **29**(1): 237-248.

Jonathan, S., et al. (2007). Metamodelling: state of the art and research challenges. he International Dagstuhl conference on Model-based engineering of embedded real-time systems. Dagstuhl Castle, Germany, Springer.

Jones, J. (2005). An Introduction to Factor Analysis of Information Risk (FAIR).

Kassab, M., et al. (2009). A Metamodel for Tracing Non-functional Requirements. Computer Science and Information Engineering, 2009 WRI World Congress on.

Kelly, C. (1998). Simplifying Disasters: Developing a Model For Complex Non-Linear Events Disaster Management: Crisis and Opportunity: Hazard

Management and Disaster Preparedness in Australasia and the Pacific Region Conference. Cairns, Queensland.

Kelly, S. and R. Pohjonen (2009). "Worst Practices for Domain-Specific Modeling." Software, IEEE **26**(4): 22-29.

Kelly, S. and R. Pohjonen (2009). Worst Practices for Domain-Specific Modeling. IEEE Software.

Khoo, Y., et al. (2001). "Motivation for ISO 14000 certification: development of a predictive model." Omega.

Kleijnen, J. P. C. and R. G. Sargent (2000). "A Methodology for Fitting and Validating Metamodels in Simulation." European Journal of Operational Research **120**: 14-29.

Kok, et al. (2010). Feature selection for fluency ranking. Proceedings of the 6th International Natural Language Generation Conference. Trim, Co. Meath, Ireland, Association for Computational Linguistics**:** 155-163.

Lagerstrom, R., et al. (2010). "Architecture analysis of enterprise systems modifiability - Models, analysis, and validation." Journal of Systems and Software.

Levendovszky , T., et al. (2010). "Model Evolution and Management, MBEERTS." Springer.

Lhoste, P. and M. Lomabard (2008). "Information modelling framework for knowledge emergence in product design."

M. Picka (2004). "Metamodelling and Development of Information System." Agriculture Economics **2**(50): 65-70.

Manning, C. D., Raghavan, Prabhakar, Hinrich (2008). Introduction to Information Retrieval. Cambridge, UK, Cambridge University Press.

March, S. and G. Smith (1995). "Design and natural science research on information technology."

Mayer, N., et al. (2009). "Design of a Modelling Language for Information System Security Risk Management ".

MYLOPOULOS, j. (1992). Conceptual modeling and Telos, Conceptual modeling, Databases and Case:An Integrated View of Information Systems Development, Wiley.

Nordstrom (1999). etamodeling - Rapid Design and Evolution of Domain-Specific Modeling Environments, Vanderbilt University. Ph.D Theses.

OMG (2001). Unified Modelling Language Specification, Object Management Group.

OMG (2002). Meta Object Facility (MOF) Specification, Object Management Group.

OMG (2003). MDA Guide Version 1.0.1.

OMG (2011). Unified Modeling Language (UML).

Othman, S. and G. Beydoun (2010). Metamodelling Approach To Support Disaster Management Knowledge Sharing. Australasian Conference on Information Systems (ACIS'2010)

Paton, D. and D. Jackson (2002). "Developing Disaster Management Capability: An Assessment Centre Approach." Disaster Prevention and Management **11**(2): 115-122.

Pidd, M. (2000). ools for Thinking - Modeling in Management Science. New York, Wiley.

Pigott, D. and V. Hobbs (2011). Complex knowledge modelling with functional entity relationship diagrams.

Roberts, J. and K. Gary (2008) The industry responds on privacy. Modern Healthcare

Rossi , M., et al. (2004). "Managing Evolutionary Method Engineering by Method Rationale." Journal of the Association for Information Systems.

Saleh, B. and F. Masseglia (2011). "Discovering frequent behaviors: time is an essential element of the context." Knowledge and Information Systems **28**(2): 311-331.

Sargent, R. G. (2005). Verification and Validation of Simulation Models. Proceedings of the 37th Conference on Winter Simulation. Orlando, Florida, Winter Simulation Conference.

Scheer (2005). "Process Modeling using Event-Driven Process Chains." Wiley.

Seidewitz (2003). "What Models Mean." IEEE Software.

SEMA (2005). Samhällets Informationssäkerhet. Swedish Emergency Management Agency. Swedish, Stockholm.

Simon, H. (1996). The Sciences of Artificial, Cambridge.

Sowa, J. F. (1984). Conceptual structures: information processing in mind and machine, Addison-Wesley Longman Publishing Co., Inc.

Sprinkle, J. M. (2003). Metamodel Driven Model Migration. Tennessee, US, Vanderbilt University. **Doctor of Philosophy:** 176

Stoneburner, G., et al. (2002). NIST Special Publication 800-30. Risk Management Guide for Information Technology Systems. Gaithersburg, National Institute of Standards and Technology.

Sturm, A. (2009). How to Choose a Metamodeling Approach. The Knowledge Industry Survival Strategy. Initiative workshop of The International Conference on Object Oriented Programming, systems, Languages and Applications (OOPSLA) Orlando. Florida USA.

Symantic (2011). Information Security yearly report

Symantic (2012). Total number of internet vulnerabilities identified, 2006-2011

Symentec.cloud (2012). Number of vulnerabilities Month-by-month 2010&2011.

Symentec.cloud (2012). Total number of internet vulnerabilities identified from 2006-2011 symentec, Symentec

Thomas, K., et al. (2003). "Model-Driven Development: A Metamodeling Foundation." IEEE.

Trabelsi, C., et al. (2011). "A Model-Driven Approach for Hybrid Power Estimation in

Embedded Systems Design." EURASIP Journal on Embedded Systems.

Vahidov, R. (2006). Proceedings of the First International Conference on Design Science Research in Information Systems and Technology

Voelter, M., et al. (2005). Model-Driven Software Engineering, Technology, Engineering, Management, John-Wiley & Sons Ltd.

Wachsmuth, G. (2007). Metamodel Adaptation and Model Co-adaptation. Proceedings of 21st European Conference on Object-Oriented Programming (ECOOP). Germany, Springer-Verlag**:** 24.

Wallin, E. and Y. Xu (2008). Managing Information Security in Healthcare. School of Economics and Managment, Lund University**:** 73.

Weilkiens, T., Ed. (2008). Systems Engineering with SysML/UML, Morgan Kaufmann Publishers Inc.

Xuan, Z., et al. (2010). Information Security Risk Management Framework for the Cloud Computing Environments. Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on.

Yan, X. and C. Lin (2010). Term-frequency Based Feature Selection Methods for Text Categorization. Genetic and Evolutionary Computing (ICGEC), 2010 Fourth International Conference on.

Zhang, Z. and N. Ye (2011). "Locality preserving multimodal discriminative learning for supervised feature selection." Knowledge and Information Systems **27**(3): 473-490.

Zschaler, S., et al. (2006). Ontologies, Meta-models, and the Model-Driven Paradigm, Springer Berlin Heidelberg.