FUZZY BASED THREAT ANALYSIS IN TOTAL HOSPITAL INFORMATION SYSTEM

NURZAINI BINTI MOHAMAD ZAIN

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

Centre for Advanced Software Engineering (CASE)
Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

OCTOBER 2009

To my Beloved Parents, Brothers & Lovely Sisters

ACKNOWLEDGEMENT

All praise be to Allah S.W.T., the Most Merciful, for His Love and Guidance. Salutations on the Prophet Muhammad (PBUH), his family, and fellow companions.

May I express my gratitude to my beloved parents and family members for being patience with me and for their love for my success.

My deepest gratitude is extended to Dr Rabiah Ahmad, for all assistance, advice, encouragement and invaluable support given as my project supervisor and as programme coordinator during my adventure in this programme. Thank you for being such a great mentor.

My sincere appreciation is given to my thesis committee panels, Prof Dr Azizah Abdul Manaf and Dr Zuraini Ismail, for their insightful comments and suggestions that were very helpful in improving the presentation of my research in this thesis. I would like to thank Mr Ganthan for his interest in my work and for providing valuable materials.

I also acknowledge my colleagues and very dear postgraduates' friends. The priceless support from Fawzia Saleh Al-Aidan, Parnian Najafi, Faiz Bashir, Orhan Argun and many others gave me strength when I thought none existed, I deeply appreciate you. Finally, special thanks are reserved for Administration personnel at the CASE and many others at UTM International Campus Kuala Lumpur for their collaboration, assistance and support.

ABSTRACT

Several studies have proposed the concept of “fuzzy logic technique" to assess risk in information security field. These studies revealed that in risk analysis process, evaluators face difficulties in collecting accurate data and adequate knowledge to estimate the probability of threats and its consequences. The estimated value contributes to data fuzziness. As a result, with the estimated value, they must make threat assessment judgment under conditions of uncertainty. Moreover, based on the literature review, there is lacks of fuzzy based threat analysis model in Healthcare Information Systems (HIS). Hence, this project attempts to develop fuzzy based threat analysis model in which; linguistic variable, fuzzy number and fuzzy weighted average are applied to deal with the uncertainty problem in doing evaluation of potential threats in Total Hospital Information Systems (THIS) environment. In fuzzification process, Triangular Average Number technique using two sets of membership functions was applied to evaluate “likelihood” and “consequence” of THIS threat variables upon a particular THIS asset. Then, each security threat level was aggregated using Efficient Fuzzy Weighted Average (EFWA) algorithm. Finally, Best Fit Technique is used in defuzzification process to translate a single fuzzy value to linguistic terms that indicates the overall security threat level impact on THIS asset. To confirm the effectiveness of this adopted model, prototype is developed and verified using scenario method. Finding shown that this model, is capable to perform threat analysis with incomplete information and uncertain in THIS environment.

ABSTRAK

Beberapa kajian telah mengutarakan konsep ‘teknik logik kabur’ untuk menilai risiko dalam bidang keselamatan informasi. Kajian-kajian ini menjelaskan bahawa dalam proses menganalisa risiko, penilai-penilai menghadapi kesukaran dari segi mengumpul data yang tepat dan pengetahuan yang mencukupi dalam menganggarkan keberangkalian ancaman-ancaman dan akibatnya. Nilai anggaran ini menghasilkan data kekaburan (ataupun anggaran). Hasilnya, berdasarkan nilai anggaran tersebut, mereka perlu membuat pertimbangan bagi penaksiran ancaman dalam keadaan ketidakpastian. Selain daripada itu, berdasarkan kajian literatur, ia menunjukkan bahawa terdapat kekurangan model penaksiran ancaman yang berorientasikan teknik kabur dalam persekitaran *Healthcare Information Systems (HIS)*. Justeru itu, projek ini berusaha mencadangkan model penaksiran ancaman berorientasikan teknik kabur di mana; pembolehubah linguistik, nombor kabur dan purata pemberat kabur digunakan untuk menangani masalah ketidakpastian dalam proses penaksiran potensi ancaman-ancaman dalam persekitaran *Total Hospital Information Systems (THIS)*. Dalam proses pengkaburan, teknik *Triangular Average Number* menggunakan dua set darjah keahlian kabur untuk menilai ‘anggaran’ dan ‘akibat’ pembolehubah ancaman *THIS* terhadap sesuatu aset *THIS.* Seterusnya, setiap tahap keselamatan ancaman dihimpunkan dengan menggunakan teknik algoritma *Efficient Fuzzy Weighted Average (EFWA)*. Akhir sekali, teknik *Best Fit* digunakan dalam proses penyahkaburan bagi menukarkan satu nilai kabur kepada terma linguistik yang menunjukkan tahap impak keseluruhan ancaman keselamatan terhadap aset *THIS.* Bagi mengesahkan keberkesanan model yang telah diubahsuai ini, prototaip dibangunkan dan disahkan dengan menggunakan kaedah senario. Hasil penemuan ujikaji menunjukkan bahawa model ini berkeupayaan membuat analisis ancaman yang melibatkan informasi yang kurang dan ketidakpastian dalam persekitaran *THIS.*

TABLES OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AHP	-	Analytic Hierarchy Process
ALE	-	Annualized Loss Expectancy
ARO	-	Annualized Rate of Occurrence
AS/NZS 4360/1999	-	Australian and New Zealand Standard for risk management
CRAMM	-	CCTA Risk Analysis and Management Method
EC	-	E-Commerce
EF	-	Exposure Factor
EFWA	-	Efficient Fixed Weightage Average
FDSS	-	Fuzzy Decision Support System
FMEA	-	Failure Mode and Effects Analysis
FST	-	Fuzzy Set Theory
FTA	-	Fault Tree Analysis
FWA	-	Fuzzy Weighted Average
GB	-	Giga Bytes
GHz	-	Giga Hertz
GUI	-	Graphical User Interface
HAZOP	-	Hazard and Operability Analysis
HFWA	-	Hierarchical Fuzzy Weighted Average
HIS	-	Healthcare Information Systems
IDE	-	Integrated Development Environment
IFWA	-	Improved Fuzzy Weighted Average Algorithm
ISO/IEC 27005	-	The International Organization for Standardization / International Electrotechnical Commission for Information Security Risk Management Standard
IT	-	Information Technology
JAR	-	Java Archive

JDBC	-	Java Database Connectivity
MB	-	Mega Bytes
MHz	-	Mega Hertz
NIST 800-30	-	National Institute of Standard and Technology -Risk Management Guide for Information Technology Systems
OCTAVE	-	Operationally Critical Threat, Asset, and Vulnerability Evaluation
PACS	-	Picture Archiving Communication System
PHA	-	Preliminary Hazard Analysis
RAM	-	Random Access Memory
ROG	-	Radius of gyration
SLE	-	Single Lost Expectancy
SQL	-	Structure Query Language
SQL	-	Structure Query Language
STRIDE	-	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege
TCP/IP	-	Transmission Communication Protocol /Internet Protocol
TCP/IP	-	Transmission Communication Protocol /Internet Protocol
THIS	-	Total Hospital Information System
VGA	-	Video Graphic Array

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

Recently, there is an increasing number of hospitals integrate Healthcare Information Systems (HIS) into their computing environment. Hence, they should be aware of the security risk associated with internal and externals threats and the impact on hospital resources and patient privacy issues (Bones *et al*., 2007). Therefore, to protect the organization information assets and its ability to perform their mission, risk management process must be carried out by the organization (NIST 800-30 Risk Management Guide for Information Technology Systems).

According to ISO/IEC 27005 Information Security Risk Management Standard, "Risk management" is the process of identifying, analyzing, evaluating, eliminating and reducing the risks of a system. Risks are weighed and decisions about acceptable risks are made. Risk analysis is part of the risk management process. The intention of risk analysis is not to help build a completely secure system, but rather to implement and maintain a correct level of security to the system. This depends on how the threats are identified. It should be correspond to the guidelines that defined prior to the analysis, which determine what is and what is not an acceptable risk.

There are many risk analysis methods. However, generally all the methods consist of four basic steps. These steps are; (a) analyze the system and its environment, (b) identify the vulnerabilities and the possible threats of the system, (c) determine the impacts and probabilities of the identified threats, and (d) evaluating the risks of the system (Xenakis *et al*., 2008).

Perceptibly, threat assessment is part of risk analysis process. Therefore, this project will examine suitable fuzzy risk analysis model and adopt the theory of fuzzy set in context of threat analysis. It seems applicable to apply this theory because threat analysis lies in theory of probability. For instance, ISO/IEC 27005 Information Security Risk Management Standard highlighted threat assessment as:

(i) Evaluating the consequences (asset value) on predefined scale of each threatened asset; and
(ii) Evaluating the probability of threat occurrence on a predefined scale of each threat.
(iii) Finally, threat can be ranked in order of their associated measure of risk.

1.1 Background of the Problem

Most risk analysis exercise lies in theory of probability and involved team effort participation. For example, a scenario is given as below:

> The threat identification was performed as a structured brainstorming between the project members and the discussion was summarized in a risk table with the following columns:
> • unique ID of threat (threat number),
> • description of threat or unwanted incidence,
> • consequence value (and additional description, if any),
> • likelihood value (and additional description, if any),
> • risk value (as a product of consequence and likelihood),
> • any other comments (including ideas for risk treatment).
>
> In the structured brainstorming process a walk-through of the architecture was performed, using predefined guidewords and attributes. Guidewords were related to the security aspects confidentiality, integrity and availability, and to attributes like “internal” and “external” (threats),

> and "deliberate" and "accidental" (actions). The risk table is non-static and is used as a tool throughout the whole process. During the brainstorming, all possible threats were written into the table, together with any relevant comments, also any comments related to consequence and likelihood. Afterwards, a clean-up of the table was performed, by grouping related threats or putting threats into a relevant sequence. At this stage each threat was given its unique ID (values for consequence, likelihood, and risk were added later on in the process).
>
> (Bones *et al*., 2007)

By considering the above scenario, obviously it seems that during the process its involved estimation values. This could lead to result of data fuzziness. Apparently, due to highly uncertainty and lack of risk analysis tool will make risk analysis exercise as daunting task. Besides, James, Ed and Mike (2008) emphasize on participation of many expert evaluator during threat assessment process that will help to produce accurate threat assessment result and stated that:

> Threats can originate from numerous sources, including IT, humans, and nature. Threat assessment should be performed as a team effort to provide the widest range of perspective. By fully evaluating risks from all angles, you reduce your system's vulnerability.
>
> (James, Ed and Mike, 2008)

1.2 Problem Statement

Recently, several researches have addressed threats existence in Healthcare Information System (HIS) environment. For instance, Ganthan, Ahmad and Ismail (2009), put emphasis on storing health information in electronic form raises concerns about patient's health, privacy and safety. In depth study, it is agreed that HIS can be threatened by both accidental events and deliberate actions threats (Maglogiannis and Zafiropoulos, 2006; Kahn and Sheshadri, 2008). As a result, these can severely damage health information systems' reliability and consequently discourage

professionals of future use. Furthermore, Ahmad *et al*. (2009) revealed that there are too many variables that can possibly occur as threats to computer system and emphasizes a need of appropriate threat analysis tools Therefore, it can be stated that prediction process in estimating the probability of threats and its consequences that take place in HIS environment is highly uncertain and crucial.

From above situations, there is a demand for a fuzzy threat analysis model and tool. Yet, the basis of this project lies in the concept of risk analysis, particularly threat assessment in the Total Hospital Information System (THIS) environment context. Therefore, a bottom line of this study is to know:

"Is fuzzy logic approach capable to perform threat analysis in healthcare information system (HIS)?"

1.3 Project Aim

Based on the above gaps, the aim of this study is to assess and analyze threat in HIS by using fuzzy logic approach. In order to verify the effectiveness of threat analysis model with fuzzy logic approach in HIS, scenario method is created based on the empirical study and data in THIS (Ganthan, Ahmad and Ismail, 2009). Furthermore, multi-expert opinion and judgment using Delphi method is applied in fuzzy threat analysis technique.

1.4 Project Objective

The objectives of this study will be as follows:

i. To investigate and determine capability of fuzzy approach in information security risk analysis. Next, a suitable fuzzy logic technique in risk analysis areas is identified.
ii. To adopt and adapt fuzzy risk analysis model and technique in developing fuzzy threat analysis model in THIS environment.
iii. To verify the fuzzy threat analysis prototype using scenario method in THIS environment.

1.5 Project Scope

This project will only focus on the development of fuzzy threat analysis model and prototype that will be validated in THIS environment using scenario method.

1.6 Summary

As HIS lies in uncertainties environment, apparently suitable fuzzy threat analysis model should be established. Furthermore, threat assessment exercise which is one of important component in risk analysis stage could helps the organization in understanding the threat they face upon the HIS resources. Consequently, appropriate steps to mitigate the THIS risks can be taken in further step. It is also foreseen that the developed model prototype can help the owner of HIS resources to perform ongoing threat assessment. This is vital in ensuring the HIS resources will be taken care of and effectively protects the patient's health, privacy and safety.

Ahmad,R., Bath,P.A., Ismail,Z., Ganthan, N.S. and Ibrahim,N.Z. (2009).Threats Identification in Healthcare Information Systems using Genetic Algorithm and Cox Regression. *5th International Conference on Information Assurance and Security (IAS-2009)*. 18-20 August, 2009. Xi'an, China :IEEE, 540-543.

Bones E, Hasvold P, Henriksen E, and Strandenaes T.(2007) Risk analysis of information security in mobile instant messaging and presence system for healthcare. IJMI 2007, 76, 677-687. Science Direct

Bouchaib, B., and Younes, B. (2004) .Information Management & Computer Security. *An exploration of wireless computing risks: Development of a risk taxonomy*.12 (3), 245 – 254.

Charette, R.N. (1989). *Software Engineering Risk Analysis and Management* (3rd ed.).McGraw-Hill, New York.

Council of Standards Australia, 1999. "AS/NZS 4360:1999 Australian Standard Risk Management". Standards Association of Australia.

Fu,Y.,Qin,Y., and Wu,X. (2008). Wireless Communications, Networking and Mobile Computing.*WiCOM '08. 4th International Conference*.12-14 October 2008. Dalian, China: IEEE, 1-4.

Ganthan,N.S. ,Ahmad,R. and Ismail,Z (2009). Security Threats Categories in Healthcare Information Systems. *Proceedings of the 14th International Symposium on Health Information Management Research (ISHIMR 2009)*. 14-16 October 2009.Kalmar, Sweden.

Huang Y.M., Kuo, Y.H., Lin, Y.T., and Cheng S.C. (2008). Toward interactive mobile synchronous learning environment with context-awareness service. *Computers & Education*, 51(3), 1205-1226. Science Direct

Huang, Y.M., Kuo, Y.H., Lin, Y.T. and Cheng, S.C.(2008).Toward interactive mobile synchronous learning environment with context-awareness service.*Computers & Education*, 51(3), 1205-1226. Science Direct

International Organization for Standardization, 2008. "ISO/IEC 27005 Information Security Risk Management Standard". ISO Publication.

Isograph Ltd (2008). Hazop+ 2008Hazard and Operability Analysis from Isograph. Retrieved January 5, 2009, from http://www.hazopstudy.com/

James, M. S., Ed, T., and Mike, C. (2008).*CISSP Certified Information Systems Security Professional Study Guide* (4th ed.). Indianapolis, Indiana. Wiley Publishing, Inc.

Kahn S and Sheshadri V. (2008). Medical record privacy and security in a digital environment. IT Pro, IEEE CS 2008; 46-52.

Katos, V., and Adams,C. (2005).Modeling corporate wireless security and privacy. *Journal of Strategic Information Systems.* 14, 307-321.

Lee,D.H. and Park,D. (1997).An efficient algorithm for fuzzy weighted average. *Fuzzy Sets and Systems*, 87(1), 39 - 45.Science Direct

Liao,Y., Ma,C. and Zhang,C. (2006). A New Fuzzy Risk Assessment Method for the Network Security Based on Fuzzy Similarity Measure. *Intelligent Control and Automation WCICA 2006 The Sixth World Congress*. Dalian, China : IEEE, 8486 – 8490

Maglogiannis I and Zafiropoulos E. (2006). Modeling risk in distributed healthcare information systems. *The 28th Annual International Conference of the IEEE on Engineering in Medical and Biology Society (EMBS)*. 30 August 2006. New York City, USA.

MySQL AB and Sun Microsystems Incorporation (2009). Using MySQL With Java. Retrieved March 13, 2009, from http://dev.mysql.com/usingmysql/java/

MySQL AB and Sun Microsystems Incorporation (2009a). MySQL 5.0 Reference Manual - 1 General Information 1.3 Overview of the MySQL Database Management System. Retrieved March 13, 2009, from http://dev.mysql.com/doc/refman/5.0/en/what-is.html

MySQL AB and Sun Microsystems Incorporation (2009b). MySQL 5.0 Reference Manual -1 General Information. Retrieved March 13, 2009, from http://dev.mysql.com/doc/refman/5.0/en/introduction.html

MySQL AB and Sun Microsystems Incorporation (2009c). MySQL 5.0. Retrieved March 13, 2009, from http://dev.mysql.com/downloads/mysql/5.0.html

MySQL AB and Sun Microsystems Incorporation (2009d). MySQL 5.0 GUI Tools. Retrieved March 13, 2009, from http://dev.mysql.com/downloads/gui-tools/5.0.html

MySQL AB and Sun Microsystems Incorporation (2009e). MySQL 5.0 Reference Manual. Retrieved March 13, 2009, from http://dev.mysql.com/doc/refman/5.0/en/index.html

National Institute of Standards and Technology (2002). 800-48. U.S Department of Ecommerce. NIST

Ngai, E.W.T. and Wat, F. K. T.(2005). Fuzzy Decision Support System for Risk Analysis in E-Commerce Development. *Decision Support Systems*, 40 (2), 235-255. Science Direct

Nguyen, H.T., and Walker, E.A. (2006). *A First Course in Fuzzy Logic*. (3rd ed.). Florida. Chapman & Hall / CRC Taylor & Francis Group.

Nilsena T., Aven,T. (2003).Models and model uncertainty in the context of risk analysis. *Reliability Engineering and System Safety*,309–317.Science Direct

Pan C. and Cai, X. (2008). A Model of Enterprise Strategic Risk Assessment:Based on the Theory of Multi-Objective Fuzzy Optimization. *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference.* 12-14 October 2008. Dalian, China: IEEE, 1-4.

Ru, W.G.D. and Eloff, J. H. P. (1996). Risk analysis modeling with the use of fuzzy logic. *Computers & Security*, 15(3), 239-248.Science Direct

Samer, F., Youssif, A., Byoung, K., Salim, H. (2008). A proactive wireless self-protection system. *ICPS '08: Proceedings of the 5th international conference on Pervasive services.* 6 – 10 July 2008. Sorrento,Italy :ACM, 11-19.

Shipley, M.F., Konin,D. A., Omer, K. (2005). Managing risks to knowledge transference in information systems: a fuzzy rule-based model. *Engineering Management Conference Proceedings. 2005 IEEE International*. 11-13 September 2005. IEEE, 564 – 568.

Shon, H. (2008).*CISSP® All-in-One Exam Guide*.(4th ed.) New York. The McGraw-Hill Companies.

Sommerville, I. (2007).*Software Engineering* (8th ed.) England. Pearson Education Limited.

Simon F. and Maria B. (2007).Advances in Fuzzy Systems: Applications and Theory — Vol. 23. Fuzzy logic for business, finance, and management (2nd Ed.), Singapore.World Scientific Publishing Co. Pte. Ltd.

Sodiya, A. S, Onashoga S.A. and Oladunjoye B.A. (2007).Threat Modeling Using Fuzzy Logic Paradigm. Retrieved January 5, 2009, from http://proceedings.informingscience.org/InSITE2007/IISITv4p053-061Sodi261.pdf

Sun Microsystems Incorporation (2009). Java SE (Standard Edition). Retrieved March 13, 2009, from http://www.netbeans.org/features/java/javase.html

Sun Microsystems Incorporation (2009a). JavaTM SE 6 and NetBeans Release Notes-Platform Installation. Retrieved March 15, 2009, from http://java.sun.com/javase/6/webnotes/install/install_jdk1.6_13-nb6.5.1.html

Sun Microsystems Incorporation (2009b). Jar File Overview. Retrieved March 13, 2009, from http://java.sun.com/j2se/1.4.2/docs/guide/jar/jarGuide.html

Sun Microsystems Incorporation (2009c). Java Downloads for All Operating Systems. Retrieved March 13, 2009, from http://www.java.com/en/download/manual.jsp

Sun Microsystems Incorporation (2009d). How do I manually download and install Java for my Windows computer. Retrieved March 13, 2009, from http://www.java.com/en/download/help/windows_manual_download.xml

Sun Microsystems Incorporation (2009e). Installing Java. Retrieved March 13, 2009, from http://www.java.com/en/download/help/index_installing.xml

Witold, P. and Fernando, G.(2007). Fuzzy Systems Engineering Toward Human-Centric Computing. (1st ed.).Hoboken, N. J.: John Wiley & Sons Incorporation.

Xenakis, C. A., Danae, P., Angeliki, S., Ioannis. (2008). Embedded and Ubiquitous Computing. *EUC '08. IEEE/IFIP International Conference*. 17-20 December 2008. Shanghai, China:IEEE, 61-68.

Xu, Z., Taghi M. K, and Edward B.A.(2003). Application of fuzzy expert systems in assessing operational risk of software Information and Software Technology, 45 (7), 373-388. Science Direct.

Zdenko, K.and Stjepan, B. (2006).Fuzzy Controller Design Theory and Applications. (1st Ed.).NW,USA.CRC Press Taylor & Francis Group

Zimmermann, H-J (1987). Fuzzy Sets, Decision Making and Expert Systems. (2nd series). USA, Kluwer Academic Publishers