ONTOLOGY FORMATION FOR PUBLICATIONS ON SOCIAL ENGINEERING

ISSAM SHAABAN MALQOUT MOSHADED AL-SHANFARI

(Matric No: 3130136)

Thesis submitted in partial fulfillment for the degree of

MASTER OF COMPUTER SCIENCE VIA MIXED MODE IN

INFORMATION SECURITY AND ASSURANCE

Faculty of Science and Technology

UNIVERSITI SAINS ISLAM MALAYSIA

Nilai

June 2015

AUTHOR DECLARATION

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

Date: June 2015

Signature:

Name: Issam Shaaban Al-Shanfari

Matric No: 3130136

Address: Malaysia
Block C- 5-32 (PALMA RAJ)
APT DESA PALMA 71800
NILAI NEGERI SEMBILAN.

BIODATA OF AUTHOR

Issam Shaaban Malqout Moshaded Al-Shanfari (3130136) was born on the 25 January 1980 in Sultanate of Oman. He is an Omani and Passport No is (03874835). He previously was a student of National College of Science and Technology which is affiliated with the University of Westminster - UK from 1999 to 2002 and graduated with a High National Diploma in computing. From 2003 to 2004 he was a student of Dhofar University and obtained Bachelor of computer science. He works as a computer technician for the ministry of education from 2003 until now. He is at present a Master student of Universiti Sains Islam Malaysia (USIM) majoring in Computer Science / Information Security and Assurance (ISA).

ACKNOWLEDGEMENT

At last, I am very glad to write this page with great thanks to Allah Almighty, who gave me the ability to complete my master's degree in Computer Science / Information Security and Assurance.

This master's thesis was written in 2014 at the Faculty of Science and Technology at Islamic Science University of Malaysia.

First of all, I wish to express my sincere gratitude to my supervisor, Dr. Roesnita Ismail, for her great support through the process of doing this thesis. I have received from her, including motivation and a lot of useful feedback. I wish her a great success in her academic career even in her different life's aspects.

It was also an honor to be able to study Information Security & Assurance at USIM University. I want to especially thank Prof. Dr. Kamaruzzaman Seman, Prof. Emeritus. Dr. Jalani Sukaimi ,Prof. Dr. Norita Norwawi, Dr. Mohammed Zalisham, Dr. Mohammad Nasrin, Dr. Najwa Alwi, Dr. Nurlida Basir, Dr. Kamarudin Bin Saadan Dr. Azni Haslizan Binti Ab Halim, Dr. Sakinah Binti Ali Pitchay for teaching me and providing me a lot of support in the field of information security.

I wish to express my debt to all of the USIM staff and all of my sincere colleagues in FST for the useful discussions we had during our study.

With my sincere thanks for the Cultural Attaché Office - Embassy of the Sultanate of Oman in KL represented in person cultural attaché Dr. Khamis Saleh Al-Bulushi and the academic adviser Dr. Ghaith Khaled Ahmed.

Finally, I dedicate this work to my sincere parents, all my family members, my wife, and my friends, for their support to me. And finally, I will not forget my home country, Oman.

ABSTRAK

Salah satu aktiviti yang signifikan ke atas bangsa pada zaman sekarang adalah bagaimana maklumat ditukar oleh pelbagai bentuk media, yang mencerminkan kepentingan perkongsian pengetahuan. Pada masa ini perkongsian pengetahuan antara objektif diperolehi secara sangat ad-hoc dan tidak mempunyai kefahaman yang sesuai makna data. Oleh itu, bagi memudahkan penggunaan semula dan perkongsian pengetahuan, ontologi mesti digunakan dalam situasi ini. Kejuruteraan sosial atau apa yang dikenali sebagai seni penembusan minda adalah koleksi teknik yang digunakan bagi memastikan orang berbuat sesuatu atau untuk mengisytiharkan tentang maklumat sulit. Kejuruteraan sosial ditakrifkan sebagai satu cara untuk mendapatkan maklumat yang bernilai mengenai sistem dari orang ramai secara umumnya, di mana-mana penyerang menggunakan sedikit maklumat yang dimiliki untuk memenangi kepercayaan mangsa, kepercayaan ini, membawa mangsa untuk memberikan maklumat sensitif kepada penyerang yang kemudiannya boleh menemui ciri-ciri sistem. Ontologi kejuruteraan sosial termasuk terjemahan dan penjelasan terma menerangkan jenis kejuruteraan sosial seperti serangan berasaskan manusia dan serangan berasaskan teknikal, ancaman, dan langkah-langkah tindakan. Peringkat-peringkat yang digunakan untuk pelaksanaan ini membentuk kaedah yang telah dicadangkan oleh Noy dan McGuiness (2000) bagi tujuan membangunkan ontologi. Kajian ini, berdasarkan penemuan dalam kesusasteraan, membangun taksonomi kejuruteraan sosial yang terdiri daripada dua kategori utama, menafsirkan penemuan dalam hierarki taksonomi dan membangunkan ontologi kejuruteraan sosial dengan menggunakan perisian 'Protégé'. Oleh itu, kajian ini bertujuan untuk menngumpul penerbitan berkaitan kejuruteraan sosial daripada pangkalan data terpilih. Kajian ini juga bertujuan untuk membangunkan koleks istilah yang berkaitan (taksonomi) berdasarkan pengekstrakan penerbitan yang berkaitan dengan kejuruteraan sosial, untuk memudahkan perkongsian maklumat dan pengetahuan serta penggunaan semula pengetahuan mengenai kejuruteraan sosial.

ABSTRACT

One of the significant activities of the nations in the present days is how information is exchanged by different forms of media, which reflects the importance of knowledge sharing. Currently this sharing of knowledge between objectives is obtained in a very ad-hoc fashion and lacks appropriate comprehension of the data meaning. Therefore, in order to facilitate the reuse and knowledge sharing, ontologies must be used in this situation. Social engineering, or what is known as the art of mind's penetration, is a collection of techniques used to make people do something or to declare about confidential information. Social engineering is defined as a way to gain valuable information about the system from people in general, where any attacker using little owned information to win the confidence of his victim, this trust, leads the victim to provide sensitive information to attacker through which can be discovered the properties of the system. The social engineering ontology includes a formal and explicit representation of the terms describing social engineering types such as human-based attacks and technical-based attacks, threats, and countermeasures. The stages used for this implementation form the methodology that has been suggested by Noy and McGuiness (2000) for the purpose of developing ontologies. This study, based on the findings in the literature, develops social engineering taxonomy consisting of two major categories, interprets the findings in a taxonomic hierarchy and develops social engineering ontology by using Protégé software. Therefore, this research aims to compile related publications on social engineering from selected databases. This study also aims to develop a collection of related terms (taxonomy) based on the extraction of publications related on social engineering, in order to facilitate information and knowledge sharing as well as knowledge reuse on social engineering.

TABLE OF CONTENTS

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES