UNIVERSITI TEKNOLOGI MARA

AN ICMPv6 THREAT MODEL

WAN NOR ASHIQIN BINTI WAN ALI

Thesis submitted in fulfillment
of the requirements for the degree of
Master of Science

Faculty of Computer and Mathematical Sciences

March 2015

CONFIRMATION BY PANEL OF EXAMINERS

I certify that a Panel of Examiners has met on 8th December 2014 to conduct the final examination of Wan Nor Ashiqin binti Wan Ali on her Master of Science thesis entitled "An ICMPv6 Threat Model" in accordance with Universiti Teknologi MARA Act 1976 (Akta 173). The Panel of Examiners recommends that the student be awarded the relevant degree. The panel of examiners was as follows:

Mazani Manaf, PhD
Associate Professor
Faculty of Computer and Mathematical Sciences
Universiti Teknologi MARA
(Chairman)

Saadiah Yahya, PhD
Professor
Faculty of Computer and Mathematical Sciences
Universiti Teknologi MARA
(Internal Examiner)

Suhaidi Hassan, PhD
Professor
School of Computing
Universiti Utara Malaysia
(External Examiner)

SITI HALIJJAH SHARIFF, PhD
Associate Professor
Dean
Institute of Graduate Studies
Universiti Teknologi MARA
Date: 16th March, 2015

AUTHOR'S DECLARATION

I declare that the work in this thesis was carried out in accordance with the regulations of Universiti Teknologi MARA. It is original and is the result of my own work, unless otherwise indicated or acknowledged or referenced work. This thesis has not been submitted to any other academic institution or non-academic institution for any other degree or qualification.

I, hereby, acknowledge that I have been supplied with the Academic Rules and Regulations for Post Graduate, Universiti Teknologi MARA, regulating the conduct of my study and research.

Name of Student : Wan Nor Ashiqin Binti Wan Ali

Student I.D. No. : 2010540059 (CS 780)

Programme : Master of Science

Faculty : Faculty of Computer and Mathematical Sciences

Thesis Title : An ICMPv6 Threat Model

Signature of Student : ....

Date : 16th March 2015

ABSTRACT

Enterprises are required to utilize Internet Control Message Protocol version 6 (ICMPv6) when IPv6 is deployed. In IPv4, Internet Control Message Protocol (ICMP) is aggressively filtered by a network administrator while in IPv6, ICMPv6 messages cannot be aggressively filtered due to the function of ICMPv6 message. ICMPv6 security risks increase when ICMPv6 threats and vulnerabilities are exploited. Thus, it is very crucial for enterprises to address the issues. In practice, network researchers must review several resources to identify ICMPv6 related attacks occurring due to the exploitation of ICMPv6 vulnerabilities. Overlooking any of these issues will jeopardize the security of ICMPv6. Currently, with the absence of ideal ICMPv6 threat model to identify and trace ICMPv6 threats, the possibility for a network to be attacked may increase. Therefore, this research aims to design and propose ICMPv6 threat model by applying the threat modeling steps. Then, attack scenario testing was conducted to validate the significance of the ICMPv6 threat model. While conducting the testing, IPv6-Filtering Prototype System (I6-FPS) was developed to overcome the deficiency and limited filtering tools that supported IPv6. I6-FPS is used to automate and simplify the writing of IPv6 filtering rules (ip6tables) and it was developed using PHP5 and Shell script languages. Overall, this research revealed that ICMPv6 threat model and I6-FPS are significant in the initial phase of securing IPv6 deployment. With the ICMPv6 threat model, enterprises are able to trace and tackle ICMPv6 threats and vulnerabilities in the IPv6 deployment. The ICMPv6 threat model has the potential to be extended by including more threats and vulnerabilities since the threat model is considered to be an iterative procedure that could be enhanced and developed over time.

ACKNOWLEDGEMENTS

بِسْــــــــــمِاللهِ الرَّحِيمِ الرَّحْمَنِ

السلام عليكم ورحمة الله وبركاته

Alhamdulillah, praise to Almighty, ALLAH S.W.T. for giving me the strength and spirit to accomplish my research.

I wish to express my sincere appreciation and gratitude to a number of people who have helped make this research a success. First and foremost, I would like to express my heartfelt gratitude to my supervisor, Dr. 'Abidah Hj. Mat Taib for her continuous support, patience, motivation, enthusiasm, and immense knowledge throughout the duration of my master study and research. Her guidance has helped me throughout the process of conducting the research and writing this thesis. I could not have imagined having a better supervisor and mentor for my master study.

Apart from my supervisor, I would also like to thank the rest of my research committee: Assoc. Prof. Dr. Naimah Mohd Hussin as my second supervisor, Mr. Raziff Rosdi, Mr. Mohammad Hafiz Ismail and Mr. Jamal Othman and other lecturers from the Faculty of Computer and Mathematical Sciences, for their encouragement, insightful comments, and enormous help.

My sincere thanks are also extended to the Ministry of Education, Malaysia for the Fundamental Research Scheme Grant (FRGS), Project Code : "600-RMI/SSP/FRGS 5/3/Fsp (54/2010)", Dana Kecemerlangan 11/2011, Project Code: "600-RMI/ST/DANA 5/3/Dst (455/2011)" and for the "Skim Latihan Akademik Bumiputera (SLAB/SLAI)" under Universiti Malaysia Perlis (UniMAP) fellowship.

I would also like to convey my deepest gratitude to my fellow labmates in Postgraduate Laboratory UiTM Perlis for the stimulating discussions, the sleepless nights we had while we were working together before the deadlines, and for all the fun we had in the last two and a half years. In particular, I am grateful to Dr. 'Abidah for enlightening me with the first glance of IPv6 research.

Last but not least, I would like to thank my family especially my mother, Wan Jahara Wan Ismail, for supporting me spiritually and emotionally throughout my life particularly as a research postgraduate student.