UNIVERSITI TEKNOLOGI MARA

RISK ASSESSMENT EQUATION FOR IPv6 NETWORK

ATHIRAH BINTI ROSLI

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

Faculty of Computer and Mathematical Sciences

August 2017

ABSTRACT

Exposure to risk due to the implementation of IPv6 has made enterprise networks take immediate actions to avoid misrepresenting of risks and applying inadequate countermeasures. Being aware of the needs to calculate the risk of IPv6 threats and vulnerabilities, enterprises demand a proper equation that is flexible to represent risks of the network. Unfortunately, the existing risk assessment equation is insufficient because it calculates risk per asset rather than the network as a whole. The current risk assessment equation also fails to relate security requirements with the dependencies of asset, threat and vulnerability. By using grounded theory, it is realized that confidentiality, integrity, and availability are important elements to be considered in risk assessment. Thus, this research proposes new risk assessment equation for IPv6 deployment that includes base score value that considers security goal of the network. The developed equation was validated via experimentation that involved testing the UDP flooding attack, TCP flooding attack and multicast attack by using OMNeT++. Result shows that the IRA6 equation is adequate in determining the risk value compared to the exvisting risk assessment equation. The risk values are associated into IPv6 threat model for future reference and as preliminary information for enterprise network. With the added information, it can be used by network administrators in their decision making and strategic planning for network security. Further research can include other elements in security goals which are nonrepudiation, authentication, authorization and accountability.

ACKNOWLEDGEMENT

In the name of Allah, the Most Beneficial and the Most Merciful. All the praises and thanks to Allah, the Lord of Al-Amin and peace upon the Master of Messager, Muhammad SAW for allowing this research to reach its completion. I am so kind heartedly would like to thank to my supervisor, Dr 'Abidah Hj Mat Taib, who gave me countless encouragement, guidance and support along the journey of completion of this research. To my second supervisor, Dr Ahmad Hanif Ahmad Baharin, for his guidance and motivational words throughout this research.

My deepest gratitude goes to my parent, Rosli Din and Hendon Sahak for their unflagging love and support throughout my life; this research is simply impossible without them. Thank you to my siblings, Al-Afiq, Asillah and Almera for their support. To all my friends, Postgraduate Lab 21 UiTM Perlis and ENAC Lab UNIMAP, thank you for your opinions and suggestions. I really appreciate the moment we shared.

This research work was supported by Ministry of Higher Education (MOHE), Malaysia and Universiti Teknologi MARA, Malaysia under Research Acculturation Grant Scheme (RAGS), Project code: "600-RMI/RAGS 5/3 (9/2014)".

Alhamdulillah and thank you.

TABLE OF CONTENTS

CHAPTER ONE
INTRODUCTION

1.1 BACKGROUND OF THE STUDY

Internet dependencies in daily routine have exposed users to security threat and this indirectly will increase the risks of cyber-attacks to the users. One of the factors that increase cyber-attacks are the inefficiency of network security in mitigating the security issue. This issue can affect client confidence, especially the Internet users. Risks to enterprise network increase especially when enterprises are connected to the local network. Exposure to the outside network such as the Internet can be dangerous because of the uncertain security measure. Moreover, network administrators possess limited control and access over major parts of the Internet that resulted in increasing rate of risks (Roy et al., 2010). When the risks increased, enterprise network needs proper approach to allow them to manage the security of their network (Ali, Taib, Hussin, Budiarto, & Othman, 2011). One of the methods that can aid the enterprise to manage their networks is by using risk assessment. Risk assessment acts to reduce risk and to identify the threat path between the enterprise resources and potential attackers (Chivers, Clark, & Cheng, 2009).

Risk assessment has been discussed for many years and there are many issues that are related to risk assessment that are being focused by the researchers. For instance, unsecured network, system analysis risk assessment, methods for risk assessment and unsolved threats are issues that need to be solved by risk assessment (Ergu, Kou, Shi, & Shi, 2014). The risk assessment inside enterprise network is vital especially when the enterprise deploys Internet Protocol version 6 (IPv6). Based on a survey conducted by BTConnect (2014), most enterprise networks do not have any mitigation strategies when they deploy IPv6. Most of them stated that it is not essential for them to apply mitigation strategies and most of them rely on Internet Service Provider (ISP) to manage their network (BTConnect, 2014). Several IPv6 features can be secret weapons for the attackers and might be a time bomb for the enterprise network (Choudhary & Sekelsky, 2010). Without suitable risk assessment, an enterprise network may be exposed to IPv6 attacks and vulnerabilities, although the intrusion detection systems have been correctly configured to deal with IPv6 traffic (Gold, 2011).