A NEW APPROACH OF NETWORK INTRUSION DETECTION SYSTEM IN 6TO4 TUNNELING

ALAUDDIN MAULANA HIRZAN

MASTER OF COMPUTER SCIENCE
(INTERNETWORKING TECHNOLOGY)

2017

Faculty of Information and Communication Technology

A NEW APPROACH OF NETWORK INTRUSION DETECTION IN 6TO4 TUNNELING

Alauddin Maulana Hirzan

Master of Computer Science in Internetworking Technology

2017

A NEW APPROACH OF NETWORK INTRUSION DETECTION SYSTEM IN 6TO4 TUNNELING

ALAUDDIN MAULANA HIRZAN

A thesis submitted
in fulfillment of the requirements for the degree of Master of Computer Science
in Internetworking Technology

Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2017

DECLARATION

I declare that this thesis entitled “A New Approach of Network Intrusion Detection System in 6to4 Tunneling” is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : ……..

Name : ……..

Date : ……..

APPROVAL

I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in terms of scope and quality for the award of Master of Computer Science (Internetworking Technology).

Signature : …….

Supervisor Name : …….

Date : …….

DEDICATION

To my late grandfather, the wisest person I have ever met

To my grandmother who cares everyone in every aspect

To my beloved mother who gives me all the support and prayers

To my respected father who always stands beside me, and many advices

To my cherished little brother who still needs to pursue his dreams

To my big family for the support and pray

To my country, Indonesia as a good and loyal citizen

ABSTRACT

Recent growth of internet users which almost reach the limit of IPv4 address space, make engineers must implement IPv6 to the system. However, the implementation of IPv6 is not easy due to many reasons like compatibility of hardware. Hence, transition mechanisms were proposed to help migration process from IPv4 to IPv6 network. However, there are security considerations of this mechanism due to the double encapsulation of packets. Basically, this mechanism encapsulates IPv6 packets with IPv4 datagram to allow transmission. Attacker from IPv6 network can use this tunneling mechanism to send intrusion without being detected by Network Intrusion Detection System. Normally NIDS only capable to decapsulate packet once, and NIDS like Snort cannot detect payload with protocol 41. Thus, a new approach is needed to handle decapsulation of second layer of packet, and extraction for the needed information for detection. This design adds a secondary decapsulation process of NIDS when NIDS detects a 6to4 packets. The design will decapsulate the second layer, and extract the information from the payload and continue to the detection process. The detection process itself is signature-based, where intrusions' unique and repetitive information are defined inside the ruleset. The design implemented to Java-based NIDS for testing purpose, and run under attack simulations. According to the test, all attacks are detected as True Positive detection with several reply packets detected as False Negative detection.

ABSTRAK

Pertumbuhan baru-baru ini daripada pengguna internet yang hampir mencapai had ruang alamat ipv4, membuat jurutera mesti melaksanakan IPv6 kepada sistem. Walau bagaimanapun, pelaksanaan IPv6 tidak mudah kerana banyak sebab seperti keserasian perkakasan. Oleh kerana itu, mekanisme peralihan telah dicadangkan untuk membantu proses penghijrahan dari IPv4 kepada rangkaian IPv6. Walau bagaimanapun, terdapat pertimbangan keselamatan mekanisme ini kerana encapsulation dua lapisan paket. Pada asasnya, mekanisme ini merangkumi paket IPv6 dengan datagram IPv4 untuk membolehkan penghantaran. Penyerang dari rangkaian IPv6 boleh menggunakan mekanisme terowong ini untuk menghantar pencerobohan tanpa dikesan oleh Network Intrusion Detection System. NIDS hanya mampu decapsulate satu lapisan paket, dan NIDS seperti Snort tidak dapat mengesan muatan dengan protokol 41. Oleh kerana itu, pendekatan baru diperlukan untuk mengendalikan decapsulation lapisan kedua paket, dan pengekstrakan maklumat yang diperlukan untuk pengesanan. Reka bentuk ini menambah proses decapsulation sekunder ketika NIDS mengesan paket 6to4. Reka bentuk akan decapsulate lapisan kedua, dan mengekstrak maklumat dari muatan dan menerusi proses pengesanan. Proses pengesanan sendiri adalah berasaskan tandatangan, di mana maklumat yang unik dan berulang-ulang pencerobohan 'ditakrifkan dalam set peraturan. Reka bentuk dilaksanakan untuk NIDS berasaskan Java untuk tujuan ujian, dan berjalan di bawah simulasi serangan. Menurut ujian, semua serangan dikesan sebagai True Positive dengan beberapa paket balasan dikesan sebagai False Negative.

ACKNOWLEDGEMENTS

I would like to express my greatest gratitude to Allah SWT. The owner of everything and the greatest in everything who gave all the guidance, love, and grace toward the author. So, the thesis entitled "A New Approach of Network Intrusion Detection in 6to4 Tunneling" can be finished on time. Therefore, I would like to express my gratitude to:

Government of Indonesia especially for Ministry of Education and Culture for Master degree scholarship to Universiti Teknikal Malaysia Melaka. To my previous university, Universitas Dian Nuswantoro for the recommendation and many supports. As well as to Universiti Teknikal Malaysia Melaka for the chance to study and learn of many things. My gratitude to: Prof. Dr. Burairah Bin Hussin as Dean of FTMK.

Dr. Wahidah binti Md Shah as Head of Department of Computer System and Communication. Dr. Nazrulazhar bin Bahaman as the supervisor of the author who help, and guide the author during experiment, and report writing. Prof. Dr. Nanna Suryana Herman as a father's figure for all Indonesian students in Universiti Teknikal Malaysia Melaka who help the author during registration and study in the university.

All lecturers in Faculty of Information and Communication Technology who gave the author knowledge and experience during study in the university. Beloved parents and families who have always provide prayer and supports. My cherished eight housemates who accompany me in sadness and laugh, solving problems together, and enjoy the risk of everything.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

The growth of communication technology increases the number of users in the network. Most of them are using IPv4 protocol to connect to internet and occupy the address space of IPv4. Since the users of IPv4 grow exponentially, soon IPv4 will not be able to allocate more address spaces for those users. Per 1st of July 2016, internet users reached 3,424,971,237 users[1], meanwhile IPv4 address pool only 4,294,967,296 addresses (2^32). That is why IPv6 is developed as a successor of IPv4 to provide more address spaces for users. However, due to many reasons IPv6 is not fully integrated to the network yet. Because of this, an approach called *6to4 tunneling protocol* (IPv6-to-IPv6-via-IPv4) implemented as solutions for IPv6 connectivity problems. This approach is one of many transition mechanisms from IPv4 to IPv6 where an explicit tunnel is established for connectivity. A network which apply this protocol usually has 6to4-configured router, and connected to IPv4 network (Bahaman et al., 2012a).

However, there are some security considerations regarding 6to4 tunneling protocol. Since 6to4 tunneling is still using IPv4 as its bridge to another network, there are big chance of attacker tries to attack or intrusions running on this protocol as medium. There are many type of network intrusions based on attack types and protocol attacks. Flooding attack such as *TCP SYN Attack* is one of most common attacks in networking. It is an attack where the

[1] http://www.internetlivestats.com/internet-users/#trend

client starts the TCP connection with the server. However, the client sends a message about requesting a connection to the server. Automatically the server will respond to the request and the client can start establishing the connection, but in this case the client keep sending and receiving the message without opening the session at all. The client keeps flooding all available connections in the server, and the result is the server deny any request from clients. These kind of intrusion is known with denial-of-service attack, where the server keep denying the traffics (Anand, 2012). If the intrusion persists and no one can stop the intrusion, then the server will overload and may cause system error or fatal crash. The worst case of this problem is data lost. Data lost occurs when the transaction within the server suddenly stopped by Denial-of-Service, and the server unable to save the current transaction session. The data which is already saved in the server storage maybe safe. However, the current transaction session maybe lost and unrecoverable. Many processes including transaction will stop, and any running queries will be cancelled. To recover data lost within the database, the administrator of the network requires a lot of time and cost as well. Hence the need for a software that can detect intrusions from inside and outside the organization.

Commented [NB1]: rephrase this sentence. Don't use "For instance"

Network Intrusion Detection System (NIDS) is developed to monitor traffic in real time, detect, and unauthorized access from third party or malicious traffic from internet or inside organization. According to (Uddin, 2016), NIDS is very practical to detect and alert the complex intrusion since firewall will not be able to hold it. Snort is one of open source network intrusion detection software to detect and prevent network intrusion. Basically, NIDS has many features such as: real time analysis, packet logging, and customizable rules to detect many intrusions. By using NIDS, users will be notified of the anomaly traffics and preparing to protect their hardware or software resources against network attacks. NIDS will analyze the traffic of the network in real time. In order to detect these presences of malicious

Commented [NB2]: Network Intrusion Detection System (NIDS)

traffic or unauthorized access, NID uses its sensors and prevent that traffic continue further to the system.

In IPv4 and IPv6 cases, NIDS able to detect intrusions easily since the packet is encapsulated one. However, 6to4 tunneling protocol encapsulates twice and make NIDS only read the IPv4 Datagram, and skip the IPv6 Datagram. Since IPv6 Datagram in this protocol is located as IPv4's payload, NIDS will let the packet go through the network to destination (P. Savola and Patel, 2004). Because of these reasons, enhancement of NIDS is needed in order to detects network intrusion inside the tunnel. According to (Bahaman et al., 2012b), there are many attacks run under 6to4 tunnel and NIDS unable to detect it. There is an experiment with NIDS in the paper, the NIDS itself is already configured by using custom rules to detect any ICMP packets in the network. The first ICMP test of IPv4 shows that the ICMP test is detected by IDS. However, the next ICMP test of IPv6 did not show any detection of intrusion. The study proves that attacks under 6to4 tunneling mechanism is undetectable by NIDS, and make IPv6 networks vulnerable toward intrusions from external networks. Thus, it is important to improve detection technique of NIDS with a new system in order to be able to detect the intrusions for future network growth.

1.2 Background of Study

The migration from IPv4 to IPv6 is still on the progress, during the migration progress 6to4 tunneling is introduced to help expanding the current network, as well as to help users and ISP to migrate to IPv6. This tunneling mechanism encapsulates any traffic from IPv6 with IPv4 encapsulation scheme, and the decapsulation process starts in the next IPv4 router. This kind of process will be useful for intrusion to hide and reach the destination passing

NIDS. This kind of issue will become a big matter in the future due to security concern in this tunneling mechanism.

This study proposes a detection mechanism to decapsulate and extract payload of incoming 6to4 packet in IPv4 networks. Once intrusion is successfully detected, it will alert and issue the report each of the intrusions into a log. A simulation will be conducted to run three different intrusions which are already selected, and detects each of them by sniffing the packet and decapsulate the packets to read the data message inside.

1.3 Problem Statement

Transition mechanism is a way to migrate IPv4 to IPv6, there are many techniques in the mechanism. 6to4 Tunneling Mechanism is one of many mechanisms that use tunneling system for IPv6 to IPv4. However this transition still has security vulnerabilities against network intrusions, and Network Intrusion Detection System (NIDS) cannot detect the intrusion in this network (Bahaman et al., 2012b). NIDS cannot detect the intrusion that flow within the 6to4 tunnel since NIDS only decapsulate the first datagram only and response the payload as normal protocol 41 that will not be detected as intrusions. Normally after the first decapsulation process, NIDS know what the next header will be. But in 6to4 tunneling case, the next header will be protocol 41, and NIDS will bypass this protocol as normal protocol. Even Snort only support certain protocols, such as TCP, UDP, ICMP, and IP[2]. The risk of data loss, or hardware failure will increase. Thus, enhancement of detection approach is important in order to make NIDS able to detect intrusions running under 6to4 tunnel.

Commented [NB3]: NIDS

[2]http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node27.html

1.4 Objective of Study

Objectives of this study are listed out as:

- To analyze network intrusion in transition mechanism approach of IPv6
- To design an approach for second decapsulation process, and a prototype of tunneling network intrusion detection system to test and evaluate the approach.
- To evaluate and validate the capability of new approach in Network Intrusion Detection System under 6to4 tunneling mechanism.

1.5 Project Scope

This study focuses on transition of IPv6 called 6to4 tunneling and attacks within this tunneling mechanism. The technology of 6to4 tunneling is implemented into a simulation. There are three kinds of attack that run during the simulation. The attacks are specialized for nodes with IPv6 that sent from other IPv6 node. And then a node will detect the presence of the attacks which are currently undetectable by any NIDS and report it into the log.

Commented [NB4]: List these attacks…

1.6 Importance of the Study

6to4 tunneling is one of transition mechanism that offered before migrating fully to IPv6. Many researchers are studying, and proposes many solutions for the tunneling performance issues instead of security issues that lied within the mechanism 6to4 has a capability to encapsulate any IPv6 packets using IPv4 datagram to allow those traffic to flow within IPv4 network. Here is the security problem of 6to4 tunneling mechanism. Intrusions in IPv6 will be encapsulated with IPv4 datagram, and remained undetectable by NIDS. Because, the current NIDS only read the first encapsulation layer and compare the payload

there with NIDS signatures. This security problem can affect network performance itself in the future.

1.7 Expected Output of Study

The result of this study will be expected to be used as network security enhancement, and especially for research studies regarding 6to4 tunneling network security. Network Intrusion Detection System detection improvement with an approach that capable to decapsulate the second layer of 6to4 packets

1.8 Conclusion

6to4 Tunneling Mechanism is one of transition mechanism of IPv6 that easy to implement for IPv6 migration to IPv4. IPv6 can be implemented right away without removing all parts of IPv4 network. This study wants to propose a new design of detection mechanism that capable to read datagram of any traffic that running in IPv4 network, and read the payload data before reaching the target. This study is expected to able detect intrusions that running in the 6to4 tunneling network, and properly write a log based on intrusions datagram before reaching target in IPv6 network.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

The security vulnerabilities in IPv6 protocol gives attacker a chance to do better intrusion in the network. In this protocol, the attacker tries to modify or intercept any flowing traffic and use them as medium to attack the nodes. Even though IPv6 offers larger address space for all internet users, security vulnerabilities still exist within the protocol and this is very risky toward users especially for enterprise level (Dawood and Jassim, 2014). Not only IPv6 protocol, dual stack protocol which is a transition mechanism that combine connectivity of IPv4, and IPv6 has this kind of risk as well. Based on (P. Savola and Patel, 2004), the characteristic of 6to4 connectivity that still use IPv4 as bridge connection between 6to4 nodes or native to 6to4 nodes makes security vulnerabilities appear. With this protocol, it is easy to do manipulation of traffic since IPv6 datagram is encapsulated in IPv4 format, especially for Denial of Service attack. However, network intrusion detection software unable to monitor this kind of protocol because of it's tunneled, and multi-encapsulation enabled (where the data encapsulated two times, the IPv4 body contains information of the IPv6 header and payload) when leaving 6to4 router to IPv4 internet, or any network that rely on IPv4 connectivity (Carpenter and Moore, 2001).

In order to make network intrusion detection software to be able to monitor, detect, and prevent intrusion in dual stack protocol, or native-6to4 network (and vice versa), enhancement is needed. The enhancement itself will make NIDS able to dismantle IP datagram of IPv4 and then dismantle the IPv6 datagram and check whether the packet is