ANALYZING IPV6 SECURITY DURING DOS ATTACK

ROSNIZA BINTI MAT SAHAK

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS TESIS

JUDUL: **ANALYZING IPV6 SECURITY DURING DOS ATTACK**

SESI PENGAJIAN:**2010/2011**

Saya **ROSNIZA BINTI MAT SAHAK**

mengaku membenarkan tesis (PSM) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hak milik UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan untuk membuat salinan tesis ini sebagai bahan pertukaran antara institusi tinggi.
4. **Sila tandakan (/)

/ SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA 1972)
TERHAD	(Mengandungi maklumat terhad yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)
TIDAK TERHAD	

(TANDATANGAN PENULIS)

Alamat tetap:No9 Parit Haji
Samsuri, Simpang Tiga,34350
Kuala Kurau,Perak

Tarikh : 4/7/2011

(TANDATANGAN PENYELIA)

En. Nor Azman bin Mat Ariff
Nama Penyelia

Tarikh : 4/7/2011

CATATAN: **Tesis dimaksudkan sebagai Laporan Projek Sarjana Muda (PSM)
**Jika tesis ini SULIT atau TERHAD,sila lampirkan surat dari pihak berkuasa

ANALYZING IPV6 SECURITY DURING DOS ATTACK

ROSNIZA BINTI MAT SAHAK

This report is submitted in partial fulfillment of the requirement for the
Bachelor of Computer Science (Computer Networking)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2011

DECLARATION

I hereby declare that this project report entitled

ANALYZING IPV6 SECURITY DURING DOS ATTACK

Is written by me and is my own effort and that no part has been plagiarized without citation

STUDENT : _____ Date: 4/7/2011
(ROSNIZA BINTI MAT SAHAK)

SUPERVISOR: _____ Date: 4/7/2011
(EN NOR AZMAN BIN MAT ARIFF)

DEDICATION

I would like to dedicate my project to supervisor, family, other lecturer and friends. This is because of their guidance and idea has contributed to the success of this project.

ACKNOWLEDGMENT

Firstly I would like to wish thank you to Encik Azman bin Mat Ariff, who is my supervisor for this final year project. He is really patient person although his student will not always come to see him to discuss about the project. He always helps me with giving some idea and notes when I have stuck with the problem that cannot be solve by me. Because of my project is done in lab, so it is hard for me to tell him about the problem of my project. Then he will come to the lab to see what the problem that he may help. It is prove that he is really concern about his student. I extremely appreciate his help so much.

Besides that, I really thankful to the university because provide me with the devices that I need for this project. The devices or the hardware that I need like four computers, one router and one switch is really expensive if I want to buy it myself. Because the university has provides all of them so I can do my project without buy anything.

My family also contributes in the success of this project. This is because they always give me support to finish my project when I feel really down. They have encouraged me to do well in this project because this is the final project that I need to settle before I graduate. They always understand me although I cannot back to the hometown during the semester break because of this project.

I also want to wish thank you to all of my friend who is always help me and accompany me at the lab. I always ask them if I do not know something and they will try their best to help me. I really appreciate their help so much. They always release my stress when I have troubled during process to finish the project. We are always help and support each other. All of this is really meaningful to me. Thank you so much.

ABSTRACT

IPv6 is introduced because of the weakness of IPv4. It has 128 bit and long enough compared to IPv4 addressing space. There has a lot of benefit of IPv6 than IPv4. One of them is IPv6 has better header format. The header of IPv6 has been designed in a way to speed-up the routing process. IPv6 also has provision for extension: It has been designed in a way that a protocol can be extended easily to meet the requirements of emerging technologies or new applications. Besides that it also has security features. IPv6 has encryption and authentication option to ensure confidentiality and packet's integrity. However, is it this security feature will make IPv6 become a secure protocol? Is it this IPv6 is secured enough to replace IPv4? This project will try to test the security of IPv6 to find the answer for each of IPv6 security issues. IPv6 network will be attack by ping flood which is one of DoS attack. How does IPv6 overcome the attack? Is it IPv6 network will down during the attack? If IPv6 is down what need to do to secure the IPv6 network? By this way, the security of IPv6 will be tested and the truth about IPv6 will be known after this project has been finish.

ABSTRAK

IPv6 diperkenalkan kerana kelemahan IPv4. Ia mempunyai 128 bitdan cukup besar berbanding alamat IPv4. Terdapatbanyak kelebihan IPv6 berbanding IPv4. Salah seorang daripadanya adalah IPv6 mempunyai *header format* yang lebih baik. *Header* IPv6 telah dicipta untukmempercepatkan proses *routing*. IPv6 juga mempunyai peruntukan untuk perkembangan. Ia telah direka untuk memenuhi keperluan teknologi dan aplikasi baru. Selain itu ia juga mempunyai ciri-ciri keselamatan. IPv6 mempunyai penyulitan dan pengesahanpilihan untuk memastikan rahsia dan integriti paket itu.Walau bagaimanapun, adakah ciri-ciri keselamatan ini akan membuat IPv6 menjadi protokol yang selamat? Adakah IPv6 ini cukup terjamin untuk menggantikan IPv4? Projek ini akan cuba menguji keselamatan IPv6 untuk mencari jawapan bagi setiap isu keselamatan IPv6. Rangkaian IPv6 akan diserang oleh *ping flood* yang merupakan salah satu serangan DoS. Bagaimanakah IPv6 akan mengatasi serangan itu? Adakah rangkaian IPv6 akan terganggu semasa serangan itu? Jika IPv6 terganggu apakah yang perlu dilakukan untuk memastikan rangkaian IPv6 selamat digunakan? Dengan cara ini, keselamatan IPv6 akan diuji dan kebenaran tentang IPv6 akan diketahui selepas projek ini telah selesai.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

IT	-	Information Technology
SMS	-	Short Message Service
FBI	-	Federal Bureau of Investigation
IC3	-	Internet Crime Complaint Center
IP	-	Internet Protocol
IPv4	-	Internet Protocol version 4
IPv6	-	Internet Protocol version 6
DoS	-	Denial of Service
TCP	-	Transmission Control Protocol
UDP	-	User Diagram Protocol
IPS	-	Intrusion Prevention System
MTU	-	Maximum Transmission Unit
RIP	-	Routing Information Protocol
ICMP	-	Internet Control Message Protocol
IPSec	-	Internet Protocol Security
LAN	-	Local Area Network
IDS	-	Intrusion Detection System

LIST OF APPENDICES

CHAPTER I

INTRODUCTION

1.1 Project Background

Nowadays, the quick development of technology occurs in many countries. There have several technologies that popular to be distributed hastily. As the example [1]the evolutions is technology in education, technology productivity tools and information technology (IT). All of them have always grown every time.

This project will focus more on IT but is usually a more general term that stresses the role of telecommunications like telephone lines and wireless signals in modern IT. It consists of all technical means used to handle information and aid communication, including computer and network hardware as well as necessary software. In other words,[2] IT consists of telephony, broadcast media, and all types of

[1] Anon (2010) .Types of Technology.[Online] Retrieve on March 2011 from http://www.muskurahatforums.com/science-arts-culture/22357-types-technology.html
[2] Anon (2011). Information and Communications Technology.[Online] Retrieve on May 2011 from http://en.wikipedia.org/wiki/Information_and_communications_technology

audio and video processing and transmission. It is prove that IT is very rapidly develop to give us easy lifestyle.

By this technology, something can be done in very short time and really low in cost. As the example, previously if we want to send a message to someone either he or she is far or near we have to write a letter. But we cannot ensure if the letter is really will receive to the right person, we do not know how much time taken to send the letter and we cannot confirms either the letter will safely delivered. At the moment, we can easily send message via email or Short Message Service (SMS) because of the technology growth.

However, there still has irresponsibility party that try to destroy our technology and make our duty become complicated. The person who is doing this activity is called as hacker.[3] Hacker is a term used by some to mean a clever programmer and by others, especially those in popular media, to mean someone who tries to break into computer systems. He defines a hacker as a clever programmer. A good hack is a clever solution to a programming problem and hacking is the act of doing it. Usually hacker will send attack to computer or system that they want to damage. This condition can be classified as cyber crime or cyber war. Cyber war is warfare in cyberspace. This includes warfare attacks against a nation's state and forcing critical communications channels and information systems infrastructure and assets to fail or destroy. This may also include warfare against foreign websites which cause the websites down and not accessible. On the other hand, cyber terrorism is the use of cyberspace to commit terrorist acts. The simple definition of cyber terrorism is the use of information technology and its means by terrorist groups and agents to cause fear or physical harm to the people.

[3] Anon (2011) "Eric Raymond, compiler of The New Hacker's Dictionary". Retrieve on June 2011 from http://rationalwiki.org/wiki/Eric_S._Raymond

1.2 Problem statement

Based on [4]Cyber Crime Statistics from the 2006 Internet Crime Report, the Internet Crime Complaint Center received and processed over 200,000 complaints. More than 86,000 of these complaints were processed and referred to various local, state, and federal law enforcement agencies. Most of these were consumers and persons filing as private persons. Total alleged dollar losses were more than $194 million. Email and websites were the two primary mechanisms for fraud. The total number of complaints decreased by approximately 7,000 complaints from 2005, while the total dollar losses increased by $15 million. The top frauds reported were auction fraud, non-delivery of items, check fraud, and credit card fraud. Top contact mechanisms for perpetrators to victims were email (74%), web page (36%), and phone (18%) (There was some overlap).

According to Cyber Crime Statistics from the 12th Annual Computer Crime and Security Survey, between 2006 and 2007 there was a net increase in IT budget spent on security. Significantly, however, the percentage of IT budget spent on security awareness training was very low, with 71% of respondents saying less than 5% of the security budget was spent on awareness training, 22% saying less than 1% was spent on such training. 71% of respondents said their company has no external insurance to cover computer security incident losses. 90% of respondents said their company experienced a computer security incident in the past 12 months. 64% of losses were due to the actions of insiders at the company. The top 3 types of attack, ranked by dollar losses, were financial fraud ($21.1 million) viruses/worms/Trojans ($8.4 million) and system penetration by outsiders ($6.8 million)

[4] Anon (2009) .Internet Crime Report. Retrieve on April 2011 from www.ic3.gov

[5]The Federal Bureau of Investigation (FBI) in collaboration with the Internet Crime Complaint Center has again published its annual report that shows cyber crime continue to be on the increase. From January 1, 2009 through December 31, 2009, the Internet Crime Complaint Center (IC3) Web site received 336,655 complaint submissions. This was a 22.3% increase as compared to 2008 when 275,284 complaints were received. Of the 336,655 complaints submitted to IC3, 146,663 were referred to local, state, and federal law enforcement agencies around the country for further consideration. The vast majority of referred cases contained elements of fraud and involved a financial loss by the complainant. The total dollar loss from all referred cases was $559.7 million with a median dollar loss of $575. This is up from $264.6 million in total reported losses in 2008. Unreformed submissions generally involved complaints in which there was no documented harm or loss or complaints where neither the complainant nor perpetrator resided within the United States

Complaints received by IC3 cover many different fraud and non-fraud categories, including auction fraud, non-delivery of merchandise, credit card fraud, computer intrusions, spam/unsolicited email, and child pornography. All of these complaints are accessible to local, state, and federal law enforcement to support active investigations, trend analysis, and public outreach and awareness efforts. On January 1, 2009, IC3 implemented a new complaint classification system based on a redesigned questionnaire that generates an automatic classification of the complaint into one of 79 offense-based categories. This redesign also resulted in a number of changes to the way the system gathers and classifies complaint data.

Significant findings related to an analysis of the complaint data include email scams that used the FBI name which is schemes in which the scammer pretended to be affiliated with the FBI in an effort to gain information from the target) represented 16.6% of all complaints submitted to IC3. Non-delivered merchandise and/or payment

[5] NeoEase (2010) FBI 2009 Cybercrime Statistic retrieve on March 2011 from http://scamfraudalert.wordpress.com/2010/03/13/fbi-2009-cybercrime-statistics/

(in which either a seller did not ship the promised item or a buyer did not pay for an item) accounted for 11.9% of complaints. Advance fee fraud (a scam wherein the target is asked to give money upfront- often times- for some reward that never materializes) made up 9.8% of complaints. Identity theft and overpayment fraud (scams in which the target is given a fraudulent monetary instrument in excess of the agreed-upon amount for the transaction, and asked to send back the overpayment using a legitimate monetary instrument) round out the top five categories of all complaints submitted to IC3 during the year.

Male complainants lost more money than female complainants (ratio of $1.51 lost per male to every $1.00 lost per female). Individuals 40-49 years of age reported, on average, higher amounts of loss than other age groups. In addition to FBI scams, popular scam trends for 2009 included hit man scams, astrological reading frauds, economic scams, job site scams, and fake pop-up ads for antivirus software.

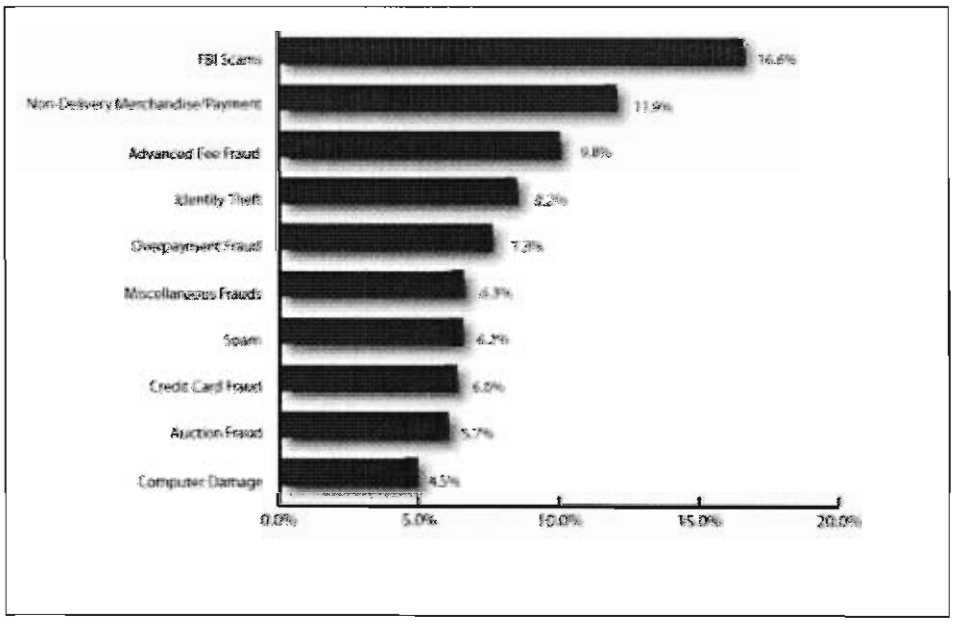

Figure 1.1: Top 10 most common complaint receive

According to Figure 1.1, it shows that the highest category that most common complaint is FBI scams. While the lowest percentage is computer damage is about 4.5%. Means that the irresponsible human love to gain information from the target than make damage to hardware.

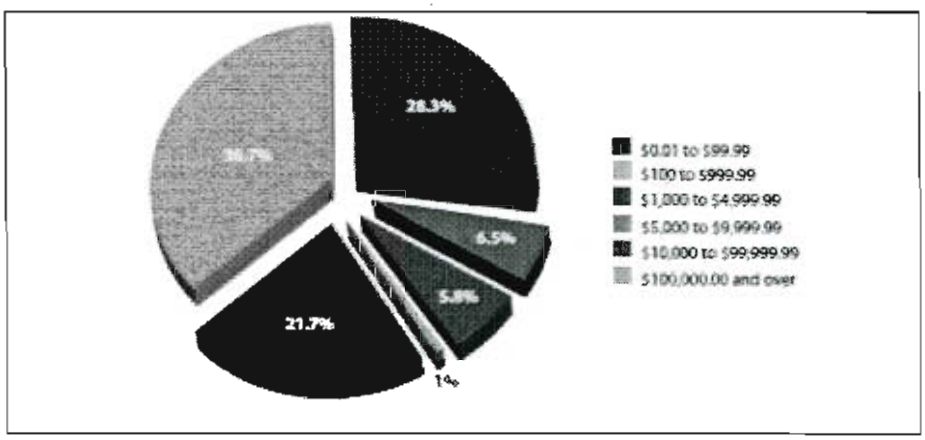

Figure 1.2: Percent of monetary loss

Based on the Figure 1.2 shows that the highest value that loss is about $1000 to $4999.99 which is 28%.While the lowest loss value is $100,000.00 and over. Although the highest loss is not much value, but the total all of them it will give a large loss.

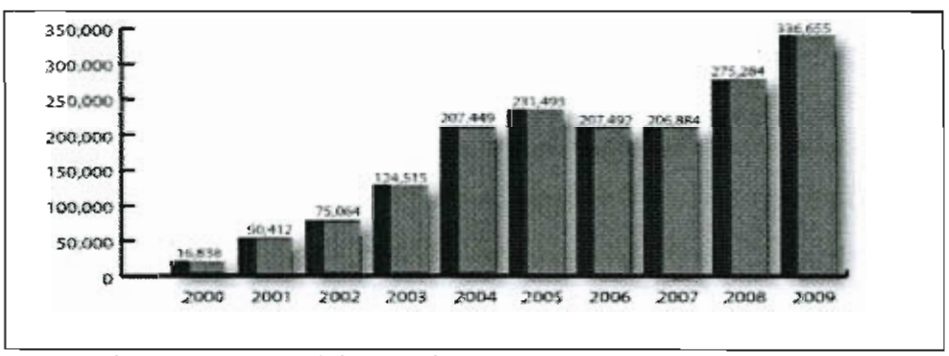

Figure 1.3: Complaint receives via website based on year.

Refer to the Figure 1.3, it shows that every year the complaint will be increase. Only on 2006 and 2007 the complaint is decrease. But it will not affect at all because only a little percent the complaint is decrease. Then on 2008 the complaint received was increase back. It show that every year the problem about the security will always increase. All of the information above is facts about cyber crime that occurs in the world. Based on statistic will see that the cyber crime is increase every year and will affect a lot of loss. There are so many methods that being used to attack or make the crime. Most people in danger because this crime is cannot be seen. Danger only can detect after the attack is happen. The best way to prevent attack must be found.

This project will focus on basic things in computer that will be important for hacker to do the crime or attack. That is Internet Protocol (IP) address which is as unique ID to recognize the host or computer. If the hacker know the IP address of a host, it will be easy to them to attack that computer. As known, the current computer still uses Internet Protocol version 4 (IPv4) as the IP address. Based on IPv4 characteristic, which is has 32 bit, it will be easy to hack the address. The IPv4 network will be really unsecured.

There are so many types of attack for IPv4 which is IP spoofing, Man in the middle attack, Server spoofing and Denial of Service (DoS) attack. Under DoS attack, there has Ping flood, ping of death and smurf. Because of the dangerousness of the attack on IPv4, the network will use Internet Protocol version 6(IPv6) on the future. It has 128 bit of IP addressing. Compare to IPv4, this IPv6 is more secure because it has large space of IP address and will be difficult to be hack. However, the attack is still can be happen. There are many types of IPv6 attack which is Denial of Service (DoS) attack, Smurf6 Attack, port scanning attack and Reconnaissance attacks.