UNIVERSITI PUTRA MALAYSIA

PRECISE ICMP TRACEBACK BASED ON NORMAL FLOW FILTRATION IN UDP/TCP SPOOFING DENIAL OF SERVICE ATTACK

ALIREZA IZADDOOST

PRECISE ICMP TRACEBACK BASED ON NORMAL FLOW FILTRATION IN UDP/TCP SPOOFING DENIAL OF SERVICE ATTACK

By

ALIREZA IZADDOOST

Thesis submitted to the School of Graduate Studies, Universiti Putra Malaysia, in fulfilment of the Requirement for the Degree of Master of Science

September 2008

To

My Beloved Mother and Sister,

and

the Soul of My Father

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Master of Science

PRECISE ICMP TRACEBACK BASED ON NORMAL FLOW FILTRATION IN DENIAL OF SERVICES ATTACK

By

ALIREZA IZADDOOST

April 2008

Chairman : Associate Professor Mohamed Othman, PhD

Faculty : Computer Science and Information Technology

In past two decades, Internet has developed rapidly and has integrated in many aspects of human life. Any disruption of connectivity and the overuse of services cause for service unavailability to its intended users. The Denial of Service (DoS) attacks are becoming more serious in security of Internet. DoS is a harmful attempt in targeting to limit or deny availability of service to legitimate users. This kind of attack can be done by consuming important resources. The best action is to block the attack traffic at its source. There is no easy way to this approach because attacker can spoof the source IP address easily.

Traceback models try to locate source of attack regardless of whether the source address field in each packet contains false information or not. Intention-driven model, a

sampling traceback technique, provides information about the attack flow and able to reconstruct the attack path to the source of attack by the aid of Intrusion Detection system (IDS). This technique does not have any flow differentiate mechanism. In other words, it is unable to differentiate legitimate user and attacker, when both of them sending packet via same route to the victim. As a result, providing incorrect information and locate false point about the source of attack.

To overcome this weakness, this research aims to increase the generation of more useful ICMP traceback packets, which includes attack path information. More useful information about the attack flow provided by the routers along the attack path to the IDS, can provide higher accuracy to locate the attacker. To achieve such a goal, this research improves the Intention-driven ICMP traceback model by filtering normal flow in the specific short time and two new algorithms in UDP-based and TCP-based attack are applied. As a consequence of filtering of normal flow, the percentage of packets belonging to the attack flow will be expanded and the chance of generating ICMP traceback messages which contain attack flow information will be increased.

The results show the proposed model used in this research increases the percentage of useful ICMP traceback messages in UDP-based attack about 10% and 14% in the TCP-based attack when compared to the previous work. The proposed model also decreases percentage of ineffective generated iTrace packets in both UDP-based and TCP-based attack about 10%.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk ijazah Master Sains

KETEPATAN MODEL JEJAK SEMULA ICMP BERDASARKAN PENYARINGAN ALIRAN NORMAL DALAM PENIPUAN SERANGAN PENAFIAN-PERKHIDMATAN UDP/TCP

Oleh

ALIREZA IZADDOOST

April 2008

Pengerusi : Profesor Madya Mohamed Othman,PhD

Fakulti : Sains Komputer dan Teknologi Maklumat

Dalam dua dekad yang lalu, Internet telah berkembang dengan pesat bertujuan melengkapi pelbagai aspek kehidupan manusia. Sebarang kehilangan sambungan rangkaian dan kegunaan yang melampau boleh menyebabkan ianya hilang keupayaan untuk memberikan perkhidmatan kepada pengguna yang terlibat. Serangan penafian-perkhidmatan (DoS) menjadi semakin serius di dalam keselamatan Internet. Serangan DoS adalah percubaan gangguan dalam mencapai had sasaran atau menafikan perkhidmatan yang boleh diperolehi oleh pengguna yang sah. Serangan jenis ini boleh dilakukan dengan menggunakan sumber-sumber yang penting. Tindakan yang terbaik ialah dengan menghalang pergerakan serangan pada punca. Tiada cara yang mudah untuk pendekatan ini kerana penyerang boleh menipu alamat sumber Protokol Internet (IP) dengan mudah.

Model-model jejak semula cuba untuk mengesan punca serangan tanpa memperdulikan

samada ruang alamat sumber dalam setiap bingkisan mengandungi maklumat yang salah atau tidak. Model *Intention-driven* adalah satu sampel teknik jejak semula yang membekalkan maklumat tentang serangan dan berupaya untuk membina semula laluan serangan kepada punca serangan dengan bantuan IDS. Teknik ini tidak mempunyai sebarang perbezaan mekanisma. Dengan kata lain, ia mampu untuk membezakan pengguna yang sah dengan penyerang, apabila kedua-dua mereka menghatar bingkisan melalui jalan yang sama kepada mangsa. Kesannya akan, memberikan maklumat yang salah mengenai punca serangan.

Bagi mengatasi kelemahan ini, objektif kajian ialah untuk menjanakan lebih banyak bingkisan jejak semula ICMP yang berguna termasuk maklumat laluan serangan. Lebih banyak maklumat yang berguna mengenai penyerang yang disumbangkan oleh penghala sepanjang laluan ke IDS, boleh mengesan penyerang dengan lebih berkesan dan tepat. Bagi mencapai matlamat ini, kajian memperbaiki model jejak semula *Intention-driven* ICMP dengan menapis aliran normal dalam masa yang singkat dan menggunakan dua algorithm baru untuk serangan terhadap perkhidmatan UDP dan TCP. Akibat daripada penapisan aliran normal, peratusan bingkisan yang dimiliki oleh aliran serangan akan meningkat dan peluang untuk menjana mesej jejak semula ICMP termasuk maklumat aliran serangan juga akan meningkat.

Keputusan ini menunjukkan model yang digunakan dalam kajian ini meningkatkan penjanaan mesej jejak semula ICMP yang berguna hampir 10% dalam serangan UDP dan 14% dalam serangan TCP berbanding dengan model yang telah sedia ada. Model ini juga telah mengurangkan peratusan bagi penghasilan bingkisan *iTrace* yang tidak

berkesan bagi kedua-dua serangan dalam perkhidmatan UDP dan TCP kepada 10%.

ACKNOWLEDGEMENTS

First and foremost I would like to express my deep gratitude to my mother for providing me the opportunity to continue my master's program and financial support. In addition, I am grateful to my supervisor Associate Professor Dr. Mohamed Othman for his kind assistance, critical advice, encouragement and suggestions during the study and preparation of this thesis. Moreover, I appreciate his encouragement to provide the opportunity to attend several conferences. I truly appreciate the time he devoted in advising me and showing me the proper directions to continue this research and for his openness, honesty and sincerity.

I would also like to express my gratitude to my co-supervisor Dr. Mohd Fadlee A. Rasid, to whom I am grateful for his practical experience and knowledge that made an invaluable contribution to this thesis.

Finally, I would like to extend my gratitude to the Dean and members of FSKTM for their endless support. Many thanks go to my caring and helpful friends, Mohamad Farhan, Ahmad Shahi and Arash Asadzadeh.

I certify that an Examination Committee has met on 3rd September 2008 to conduct the final examination of Alireza Izaddoost on his Master of Science thesis entitled "Precise ICMP Traceabck Based on Normal Flow Filtration In UDP/TCP Spoofing Denial of Service Attack" in accordance with Universiti Pertanian Malaysia (Higher Degree) Act 1980 and Universiti Pertanian Malaysia (Higher Degree) Regulations 1981. The Committee recommends that the candidate be awarded the relevant degree. Members of the Examination Committee are as follows:

Rusli Abdullah, PhD
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Abdul Azim Abd. Ghani, PhD
Associated Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Nur Izura Udzir, PhD
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Abdul Hanan Abdullah, PhD
Professor
Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia
(External Examiner)

_____

HASANAH MOHD GHAZALI, PhD
Professor/Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia
Date:

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirements for the degree of Master of Science.
Members of the Supervisory Committee were as follows:

Mohamed Othman, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Mohd Fadlee A. Rasid, PhD
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

_____

AINI IDERIS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 13 November 2008

DECLARATION

I declare that the thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously and is not concurrently submitted for any other degree at UPM or at any institution.

_____

Alireza Izaddoost

Date:

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACK	Acknowledgment
BGP	Border Gateway Protocol
CBR	Constant-Bit-Rate
CERT	Computer Emergency Response Team
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
DPM	Deterministic Packet marking
FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Medium Access Control
OS	Operating System
Otcl	Object Tcl
PPM	Probabilistic Packet Marking
RFC	Request For Comments
RTT	Round Trip Time
SYN	Synchronies
TCP	Transmission Control Protocol
TFN	Tribal Flood Network
TTL	Time To Live
TVL	Tag-Length-Value
UDP	User Datagram Protocol

CHAPTER 1

INTRODUCTION

In the past two decades, the Internet has developed rapidly and has integrated in many aspects of human life. The Internet is a vast array of connected networks situated all over the world, easily accessible by individual computer host in a variety of ways. Today people use a wide range of sophisticated Internet service application in their daily lives such as search engines, online banking, online trading, e-commerce, etc. Individuals and organizations worldwide can reach any point on the network without regarding to national or geographic boundaries or time of day. As such the widespread usage of Internet without a doubt has become a critical part of today's life. However, as more activities relay heavily on the networked computers and Internet, along with the convenience and speed of access to information, come new risks. Among them are the risks that valuable information will be lost, stolen or corrupted. Thus securing the Internet infrastructure has become the highest concern [18].

In recent years, Denial of Service (DoS) attacks are becoming more serious in security of Internet. DoS is a harmful attempt in targeting to limit or deny availability of service to legitimate users. This kind of attack can be done by consuming important resources as well as network bandwidth, server memory, disk space, or CPU time and to block access from normal users. From December 2005 to January 2006, 1500 separate IP addresses became victims of attacks, with some attacks using traffic rates as high as 10 Gbps [29].

TCP/IP lacks the security features that make it easy for IP spoofing during DoS attack. Traceback technique is suggested in finding the real source of attack and this technique is able to reconstruct the attack path, and locate the attacker. Identifying the sources of attack packets is the first step in making attackers accountable. In addition, figuring out the network path, which the attack traffic follows, can improve the efficacy of defense measures, such as packet filtering [29].

This thesis presents a discussion about the current research in traceback area and presents two different techniques in attack source identification in the UDP or TCP DoS attack.

1.1 Background and Motivation

As the Internet grows in size and complexity, its availability to different kind of attacks has been increased. Various types of attacks can happen, for example in *Buffer over flow*, attacker takes advantages by inserting his code into a program and then takes control of the system and thus the program error causes the buffer to overflow. In *Malware attacks*, an attacker uses malicious software, such as worms, viruses and Trojan horses. Attacker aims to put harmful software to create a host of problems, which can range from simple problems to even getting accesses to the computer at a later time. In *Denial of service attack*, attacker attempts to stop legitimate users from getting access to network resources. It can take place by flooding the network or server with huge useless traffic [18].

Network security considers three main goals: 1) *Confidentiality*: ensure data is kept private. 2) *Integrity*: data must be protected from unauthorized modification whether by human error or intentional tampering. 3) *Availability*: guarantee access to data be available as needed [18]. DoS attack causes problems in availability of data when it is needed.

DoS attack can be listed into two main categories: ordinary and distributed. In the ordinary DoS attack class, attacker uses a tool to sends packets to the target system. These packets are intended to disable or overwhelm the victim, usually to reboot the target. In the Distributed DoS (DDoS), attacks will emerge from many places called zombies or agents. DDoS can disable the servers, and block the legitimated users to access the resources [7].

IP spoofing is commonly linked with malicious network activities, such as DoS/DDoS attacks [43]. Each IP packet contains two addresses: source and destination. The destination address is used by the routing architecture to deliver the packet. The IP network routing infrastructure does not verify the authenticity of the source address carried in IP packets. In general, no entity is responsible for the correctness of source address. The source address is needed by the destination for the message reply [30]. DoS/DDoS attacking tools spoof IP addresses by randomizing the 32-bit source-address field in the IP header, which hides attacking sources.

An action to identify the real source of attack packets is the traceback method. The advantage of this method is the attacker is held accountable for abusing the Internet. In

addition it is useful in reducing DoS attacks either by isolating the identified attack sources or by filtering attack packets as mentioned in [3].

In the literature relating to DoS, several traceback techniques are suggested and they are still under additional research [5, 6, 33, 44]. One of these methods is ICMP traceback model which generates and sends out-band ICMP traceback messages. Generated traceback packets include enough information for the victim to use them to rebuild the attack path [6]. This method is explained in details in chapter 4. This research improves Intention-driven iTrace model [44] in order to locate the source of attack as accurate as possible.

1.2 Problem Statement

Traceback methods have been suggested as a source-spoofed IP packet detection in DoS. In the traceback model, partial information about the path is provided to the victim or to Intrusion Detection System (IDS). After collecting enough information about the attack path, victim can make a reverse chain to the source of attack. ICMP traceback and Intention-driven ICMP traceback are two models belonging to traceback methods. Intention-Driven iTrace model, an enhanced model of ICMP traceback, can provide more "useful" traceback packets to the victim to reconstruct the path compared to original ICMP traceback model.

The meaning of "useful" ICMP traceback (called iTrace) is a packet whereby information provided is related to the attack path and by providing this information, the victim would be able to reconstruct the path to the source [44].

When the attack flow and legitimate flow send packets to the same destination (victim), generated iTrace and information provided in some routers along the path has a significant effect in finding the accurate source. We define this router with an important task to provide correct information about attack path labels as *critical routers.*

However, Intention-driven iTrace model lacks of flow differentiate mechanism cause a serious problem. In other words, it is unable to differentiate legitimate user and attacker, when both of them sending packet via same route to the victim. This problem makes the critical routers provide incorrect information and locate false point about the source of attack.

1.3 Research Objective

The objectives of this thesis are:

- To propose a new algorithm in *UDP-based* DoS attack.
- To propose a new algorithm in *TCP-based* DoS attack.

These two new algorithms increase the percentage of useful iTrace packets. These packets are generated by the critical routers along the attack path which provide more useful information about the accuracy of attack location.

1.4 Research Scope

This research focuses on traceback method in DoS in ordinary attack class [7]. Our traceback model aims to locate real attacker and not the zombies or agents associated in distributed class of DoS attack. DDoS is a distributed model of DoS and proposed