
UNIVERSITI PUTRA MALAYSIA

# ENHANCED IP SPOOFING DEFENSE THROUGH CLUSTERED INTERDOMAIN PACKET FILTERING STRATEGY

LEE SOON

FSKTM 2011 18

# ENHANCED IP SPOOFING DEFENSE THROUGH CLUSTERED INTERDOMAIN PACKET FILTERING STRATEGY

**LEE SOON**

**MASTER OF SCIENCE**
**UNIVERSITI PUTRA MALAYSIA**

**2011**

# ENHANCED IP SPOOFING DEFENSE THROUGH CLUSTERED INTERDOMAIN PACKET FILTERING STRATEGY

**BY**

**LEE SOON**



**Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirements for the Degree of Master of Science**

**September 2011**

To my parents, brother and sister

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

**ENHANCED IP SPOOFING DEFENSE THROUGH CLUSTERED INTERDOMAIN PACKET FILTERING STRATEGY**

By

**LEE SOON**

**September 2011**

**Chair : Professor Mohamed Othman, PhD**

**Faculty : Computer Science and Information Technology**

In current Internet communication world, validity of the source of Internet Protocol packet is an important issue. The problems of IP spoofing alarm legitimate users of the Internet. Various spoofing defenses techniques and mechanisms are proposed by researchers, among which, Interdomain Packet Filter (IDPF) architecture proposed by Duan, et al. is promising. Based on the information from Border Gateway Protocol (BGP), IDPF is constructed. Filtering nodes are chosen based on vertex cover of the graph. This thesis presents a clustered strategy for selection of filtering nodes for IDPF architecture. Clusters of filtering nodes are chosen from the Autonomous System with highest number degree. Through analysis and simulation, the effectiveness of IDPF with Clustered Filtering was measured. The work presented here has profound implications for future studies of IP spoofing defense under IDPF.

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

**PENINGKATAN PERTAHANAN PERMALSUAN PROTOKOL INTERNET MELALUI STRATEGI PENAPISAN PAKET KLASTER ANTARA DOMAIN**

Oleh

**LEE SOON**

**September 2011**

**Pengerusi : Profesor Mohamed Othman, PhD**

**Fakulti : Sains Komputer dan Teknologi Maklumat**

Dalam dunia komunikasi Internet saat ini, kesahihan sumber paket Internet merupakan isu penting. Masalah pemalsuan paket Internet telah menggera pengguna sah lain dari Internet. Pelbagai teknik dan mekanisme pertahanan terhadap pemalsuan paket Internet telah diajukan oleh para penyelidik, di antaranya, senibina penapis paket antara domain (IDPF) dicadangkan oleh Duan, dll amat memberangsangkan. IDPF dibina berdasarkan maklumat dari protokol batas pintu gerbang. Nod penapisan dipilih berdasarkan penutup mercu graf. Tesis ini menunjukan pemilihan nod penapis senibina IDPF berdasarkan strategi berkelompok. Nod klaster penapis dipilih daripada sistem autonomi dengan sambungan nod tertinggi. Melalui analisis dan simulasi, keberkesanan IDPF dengan penapisan berkelompok diukur. Kerja yang disampaikan dalam tesis ini mempunyai implikasi besar untuk kajian masa depan dalam pertahanan pemalsuan paket Internet di bawah IDPF.

**ACKNOWLEDGEMENTS**

I would like to thank every one that helps me to accomplish my master research in University Putra Malaysia. Firstly I would like to thank Prof. Dr. Mohamed Othman for his patient and advices guiding me throughout this research. I would also like to take this opportunity to convey my highest appreciation to thank my parents for giving me courage and support. I really appreciate all the guidance and advices given by them throughout the research. I would like to thank my friends Tareq Rasul and Nazmin, and all those I've not mentioned. Thank you for all you supports and helping hands.

I certify that an Examination Committee has met on date of viva voce to conduct the final examination of name of student on his (or her) degree thesis entitled "Title of thesis" in accordance with Universiti Pertanian Malaysia (Higher Degree) Act 1980 and Universiti Pertanian Malaysia (Higher Degree) Regulations 1981. The Committee recommends that the student be awarded the (Name of relevant degree).

Members of the Examination Committee were as follows:

**Abdul Azim Abd Ghani, PhD**
**Professor**
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

**Name of Examiner 1, PhD**
Title (e.g. Professor/Associate Professor/Ir) – omit if irrelevant.
Name of Faculty
Universiti Putra Malaysia
(Internal Examiner)

**Name of Examiner 2, PhD**
Title (e.g. Professor/Associate Professor/Ir) – omit if irrelevant
Name of Faculty
Universiti Putra Malaysia
(Internal Examiner)

**Name of External Examiner, PhD**
Title (e.g. Professor/Associate Professor/Ir) – omit if irrelevant
Name of Department and/or Faculty
Name of Organisation (University/Institute)
(External Examiner)

_____

BUJANG KIM HUAT, PhD
Professor and 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 fulfilment of the requirement for the degree of type of degree. The members of the Supervisory Committee were as follows:

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

**Nur Izura Udzir, PhD**
Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)



_____

**BUJANG BIN KIM HUAT, PhD**
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

## DECLARATION

I declare that the thesis is 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 Universiti Putra Malaysia or at any other institution.

_____

**LEE SOON**

Date: 8 September 2011

## TABLE OF CONTENTS