UNIVERSITI PUTRA MALAYSIA

DETECTION OF DENIAL OF SERVICE ATTACKS AGAINST DOMAIN NAME SYSTEM USING NEURAL NETWORKS

SAMANEH RASTEGARI

DETECTION OF DENIAL OF SERVICE ATTACKS AGAINST DOMAIN NAME SYSTEM USING NEURAL NETWORKS

By

SAMANEH RASTEGARI

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

August 2009

DEDICATION

This thesis is dedicated to my wonderful parents who have raised me to be the person I am today. Also, this thesis is dedicated to my fiancé, Mohsen Meysami, who has been a great source of motivation and inspiration.

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

DETECTION OF DENIAL OF SERVICE ATTACKS AGAINST DOMAIN NAME SYSTEM USING NEURAL NETWORKS

By

SAMANEH RASTEGARI

August 2009

Chairman: **M. Iqbal Saripan, Phd**

Faculty: **Engineering**

Along with the explosive growth of the Internet, the demand for efficient and secure Internet Infrastructure has been increasing. For the entire chain of Internet connectivity the Domain Name System (DNS) provides name to address mapping services. Hackers exploit this fact to damage different parts of Internet. In order to prevent this system from different types of attacks, we need to prepare a classification of possible security threats against DNS.

This dissertation focuses on Denial of Service (DoS) attacks as the major security issue during last years, and gives an overview of techniques used to discover and analyze them.

The process of detection and classification of DoS against DNS has been presented in two phases in our model. The proposed system architecture consists of a statistical pre-processor and a machine learning engine.

The first step in our work was to generate the DNS traffic in normal and attack situations for using as the input of our intrusion detection system (IDS). With the prior knowledge of DoS attacks against DNS, we used a network simulator to model DNS traffic with high variability. Therefore, the difficulty of creating different scenarios of attacks in a real environment has been decreased. The pre-processor, processes the collected data statistically and derives the final variable values. These parameters are the inputs of the detector engine.

In the current research for our machine learning engine, we aimed to find the optimum machine learning algorithm to be used as an IDS. The performance of our system was measured in terms of detection rate, accuracy, and false alarm rate. The results indicated that the three layered back propagation neural network with a 3-7-3 structure provides a detection rate of 99.55% for direct DoS attacks and 97.82% for amplification DoS attacks. It can give us 99% accuracy and an acceptable false alarm rate of 0.28% comparing to other types of classifiers.

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

PENGESANAN SERANGAN PENAFIAN PERKHIDMATAN KE ATAS SISTEM NAMA DOMAIN MENGGUNAKAN RANGKAIAN NEURAL

Oleh

SAMANEH RASTEGARI

August 2009

Pengerusi: M. Iqbal Saripan, Phd

Fakulti: Kejuruteraan

Selari dengan peningkatan penggunaan internet, permintaan kepada infrastruktur internet yang cekap dan selamat kian bertambah. Satu sistem yang dinamakan *Sistem Nama Domain* (DNS) digunakan untuk membekalkan nama bagi perkhidmatan pemetaan alamat untuk setiap rangkaian perhubungan melalui Internet, Penggodam komputer mengeksploitasi maklumat ini untuk kepentingan mereka. Bagi menghalang sistem Internet daripada sebarang bentuk serangan, satu klasifikasi mengenai sebarang kemungkinan yang membawa kepada ancaman terhadap keselamatan DNS harus disediakan.

Tesis ini memfokuskan tentang serangan-serangan penafian perkhidmatan ke atas (DoS) kerana serangan DoS merupakan isu yang paling utama sejak beberapa tahun kebelakangan ini. Hasil kajian ini juga memberi satu gambaran secara menyeluruh mengenai teknik-teknik yang boleh digunakan untuk mencari dan menganalisa mereka.

Di dalam model kami, proses mengesan dan membezakan DoS berbanding DNS dilaksanakan dalam dua fasa. Sistem binaan yang dicadangkan merangkumi prapemprosesan secara statistik dan juga enjin pembelajaran mesin.

Langkah pertama yang dilaksanakan dalam kajian kami ini adalah menghasilkan trafik DNS dalam situasi yang normal dan juga situasi serangan dimana ianya akan digunakan semula sebagai input kepada sistem pengesan penceroboh (IDS). Berpandukan kepada serangan-serangan DoS terhadap DNS yang terdahulu, perisian simulasi rangkaian digunakan untuk membina model trafik DNS dengan pelbagai pemboleh ubah. Dengan ini, kesukaran mencipta senario serangan yang berbeza-beza dalam persekitaran sebenar dapat dikurangkan. Prapemproses memproses semua data-data statistik yang terkumpul dan menentukan nilai akhir bagi sesuatu pemboleh ubah. Parameter-parameter ini adalah input kepada enjin pengesan.

Dalam kajian ini, kami mensasarkan satu algoritma pembelajaran mesin yang optimum bagi kegunaan IDS. Prestasi sistem disukat dari segi kadar pengesanan, ketepatan pengesanan, dan juga kadar salah kesan(false alarm). Keputusan kajian menunjukkan rangkaian neural rambatan balik tiga lapisan berstruktur 3-7-3 memberi kadar pengesanan sebanyak 99.55% bagi serangan DoS secara langsung dan sebanyak 97.82% bagi serangan DoS berganda. Teknik ini memberikan ketepatan sehingga 99% dan kadar salah kesan pada nilai yang boleh diterima iaitu 0.28% berbanding teknik pengkelasan yang lain.

ACKNOWLEDGMENT

I would like to express my deep and sincere gratitude to my supervisor, Dr. M. Iqbal Saripan, Lecturer of the Department of Computer and Communication Systems Engineering, Faculty of Engineering, Universiti Putra Malaysia. His wide knowledge and his logical way of thinking have been of great value for me. His understanding, encouraging and personal guidance have provided a good basis for the present thesis. I also wish to thank Dr. Mohd. Fadlee A. Rasid, Head of the Department of Computer and Communication Systems Engineering, for his valuable advice. His extensive discussions around my work and interesting explorations in operations have been very helpful for this study.

I wish to extend my warmest thanks to all those who have helped me with my work in the Department of Computer and Communication Systems Engineering and Multimedia Laboratory.

I owe my loving thanks to my mother, Shamsi Moshtashfi pour, and my fiancé, Mohsen Meysami. They have lost a lot due to my research abroad. Without their encouragement and understanding it would have been impossible for me to finish this work. My special gratitude is due to my father, my brothers, my sister, and my dear friend, Nesa Mouzehkesh, for their loving support.

The financial support of the Universiti Putra Malaysia is gratefully acknowledged.

Universiti Putra Malaysia, Malaysia, April 2009

Samaneh Rastegari

APPROVAL

I certify that an Examination Committee has met on …….. to conduct the final examination of Samaneh Rastegari on her Master of Science thesis "Detection of Denial of Service Attacks Against Domain Name System Using Neural Networks" 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:

NOR KAMARIAH BT. NOORDIN, PhD
Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

AHMAD FAUZI ABAS, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

MOHD. HAMIRUCE MARHABAN, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

AZURALIZA ABU BAKAR, PhD
Associate Professor
Faculty of Technology and Information Science
Universiti Kebangsaan Malaysia
(External Examiner)

Bujang Kim Huat, PhD
Professor and Deputy Dean
School Of Graduate Studies
University Putra Malaysia

Date:

This thesis submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Science. The members of the Supervisory Committee were as follows:

M. Iqbal Saripan, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

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

HASANAH MOHD GHAZAL, PhD
Professor and Dean
School Of Graduate Studies
University Putra Malaysia

Date: 10 December 2009

DECLARATION

I hereby 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 or concurrently submitted for any other degree at UPM or other institutions.

_____

SAMANEH RASTEGARI

Date:

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

DNS	Domain Name System
ICANN	Internet Corporation for Assigned Name and Numbers
UDP	User Datagram Protocol
IDS	Intrusion Detection Systems
DoS	Denial of Service
SANS	SysAdmin, Audit, Network, Security Institute
TLD	Top-Level Domain
SLD	Second-Level Domain
OUSPG	Oulu University Secure Programming Group
ISC	Internet Software Consortium
NISCC	National Infrastructure Security Co-ordination Centre
ISP	Internet Service Provider
SSAC	Social Security Advisory Committee
EDNS	Extension Mechanisms for DNS
SAVE	Source Address Validity Enforcement protocol
HIDS	Host-Based IDS
NIDS	Network-Based IDS
NNIDS	network-node based IDS
ML	Machine Learning
HIDE	Hierarchical Intrusion Detection
BP	Back propagation

PBH	Perceptron-back propagation-hybrid
RBF	Radial Basis Function
MLP	Multi Layer Perceptron
SOM	Self Organizing Maps
SVM	Support Vector Machine
FL	Fuzzy Logic
DLL	Dynamic-link library
CBR	Constant Bit Rate
RNG	Random Number Generation
TP	True Positive
TN	True Negative
FP	False Positive
FN	False Negative
FAR	False Alarm Rate
MSE	Mean Squared Error

CHAPTER 1

INTRODUCTION

1.1 Background

The Internet carries various information resources and services such as electronic mail and file transfer. Today people use the Internet for remote learning, online marketing and e-banking for easier and more flexible communication. Alarmingly, however, it is easy to predict the web of tomorrow will support billions of users and more sophisticated applications will be required. Therefore, with the increased potential for the communication, the demand for Internet security is increasing as well.

The Domain Name System (DNS) is one of the important elements of this infrastructure which provides a fundamental service for end users. In order to make a successful Internet connection, name to address mapping services should be provided by DNS. In the point of fact, the name resolution mechanism operates based on a distributed hierarchical database of computers, services or any resources participating in the Internet. Currently, the Internet Corporation for Assigned Name and Numbers (ICANN) is managing the DNS to ensure that every address is unique. Originality DNS was designed based on an unreliable delivery protocol named User Datagram Protocol (UDP) and security of DNS was not a big issue at that point in time because the original design was sufficient to satisfy the needs of the Internet [Davidowicz. 1999][Chatzis. 2007]. Nowadays, DNS has become a vital service for the operation of the Internet and of any private network of a certain size so this is the time to secure the DNS system from any unauthorized access.

DNS uses two elements for the whole process of the name resolution: name server and resolver. Basically, DNS is a global connected network of "name serves" and the interaction between a DNS server and a client is based on a software that is implemented in hosts called "resolver". Any security threats against these two components can interrupt the running of the Internet.

Nowadays, organizations are increasingly implementing various Intrusion Detection Systems (IDS) to reach network security. An IDS is a defence system which detects suspicious behaviour in the network. There were several attempts to propose a solution to defend DNS against attacks [Wang, et al. 2006, Kambourakis, et al. 2007] which will be explained more in the literature review, but according to our knowledge, there was no specific intelligent detection system for Denial of Service (DoS) threats against DNS and this is the focus of this work. Having such a system beside other existing countermeasures will succeed in securing the whole network from any type of attacks.

1.2 Problem Statement and Motivation

DNS is the main port of entry between the network and the outside world, and as such, it is often the first point of attack from hackers. Managing and maintaining DNS is a challenge for any organization. The network administrators of such organizations try to address security threats against DNS to have greater controls over their systems.

According to SANS (SysAdmin, Audit, Network, Security) institute security reports, DNS servers have been appeared in the Top-20 Internet security attack target list for

seven consecutive years because of recursion DoS attacks and spoofing authoritative zone answers [SANS Institute. 2006]. Examples of the attacks are as follows:

1. In October 2002, a massive distributed reflected DoS attack targeted eight out of thirteen root DNS servers. In 2003 and 2004, other similar attacks suffered DNS badly [Steve. 2002].
2. In February 2006, payment-processing company StormPay website was kept offline for several days. A distributed DoS attack involving DNS amplification flooded StormPay with up to 6 Gbps of space. The attackers exploit bogus DNS requests to cause Internet name servers to overload StormPay's website with traffic [Department of Homeland Security. 2006].
3. In February 2007, a significant distributed DoS attack from more than a thousand computer units on the Internet flooded several servers including the U.S. Department of Defense's G server [ICANN. 2007].

It is very critical for network administrators to identify the variety of attack techniques in order to overcome them. Though many researches have been done to address different DNS security threats and evaluate the countermeasures against them, none of them are complete, simply because the variety and the quality of attack techniques may thrive. However, we believe that based on the current situation there is a need for a guiding framework including taxonomy of security attacks against DNS. This motivates us to study the security threats against DNS during recent years and make an attack tree of them to accomplish the security mechanisms for countering these threats.

Another challenge in this area is to provide an effective defense mechanism to detect DoS attacks as the major security issue during last years. Several researchers have intensively studied DNS-related Internet threats and introduced several countermeasures to overcome these threats [Chatzis. 2007, Vaughn, et al. 2006, Molsa. 2005, Aina, et al. 2006, Cheung. 2006]. However, further attempts are necessary since the existence of system vulnerabilities is unavoidable in case of coming the new attackers and new tactics. Nowadays, DNS name servers are suffering from the lack of an effective intrusion detection system. The aforementioned challenge also motivates us to study the current proposed detection systems and their ability of learning new attacks and then implement an effective detection system on DNS servers with high detection rate.

Within the last years, using commercial IDS technologies have been grown rapidly. INSECURE.ORG [Insecure.Org. 2006] listed the top 5 IDSs which are Snort, OSSEC HIDS, Fragroute, BASE, and Sguil. Snort as the most popular one is as open source IDS which can detect thousands of worms, vulnerability exploit attempts, port scan, and other suspicious behaviors by protocol analysis, content searching, and various preprocessing. It is designed based on a rule-based system and a modular detection engine.

1.3 Aim and Objectives

The aim of this thesis is to detect DoS attacks against DNS system using neural networks.

In order to achieve the aim, we have defined our research objectives as follows:

1. To modify network simulator NS-2 to support DNS system.
2. To generate different DoS attacked data using the modified NS-2.
3. To develop an effective model using several machine learning algorithms.

1.4 Thesis Scope

This thesis presents a detection system for DoS attacks against DNS. Two defined classes of DoS against DNS are direct DoS and reflected DoS. The system has the ability to classify the type of attacks. Our research focus in this thesis is on a major security threat against DNS which is DoS attack. Along with classification, the function of blocking different attacks will be simplified. It facilitates developing defence mechanisms for researchers. For the purpose of classifying DoS attacks, several features are used as classification criteria.

The main task of each security system is to detect an attack at first, and then try to repel it. Our model is designed for the first phase of a defence system to detect possible DoS attacks against DNS. The next step for specific block functions is administrator based and is not in the scope of this research. Blocking function is done by taking advantage of additional countermeasures, for example: specific block functions to terminate sessions, backup system, routing connections to a system trap, legal infrastructure, etc.

The summary of the direction taken in this project is illustrated in Figure 1.1. This thesis followed the bold texts and lines. As already mentioned, this thesis attempts to find a structured mechanism to reactively detect DoS threats against DNS. Since malicious DNS DoS attacks are in the wide group of network intrusions, this system

will be categorized as an IDS. Depending on the information source which in this thesis is the network traffic received by the targeted name server, our IDS is a combination of host based and network based which has been named network-node based IDS (NNIDS). This IDS takes advantage of the anomaly detection approach which sometimes referred to as behaviour based. Focusing, thus, on anomaly based NNIDS technologies; we stick to the machine learning schemes for categorizing analyzed patterns. This thesis tries to develop an effective machine learning based model and evaluates the performance of different machine learning algorithms.

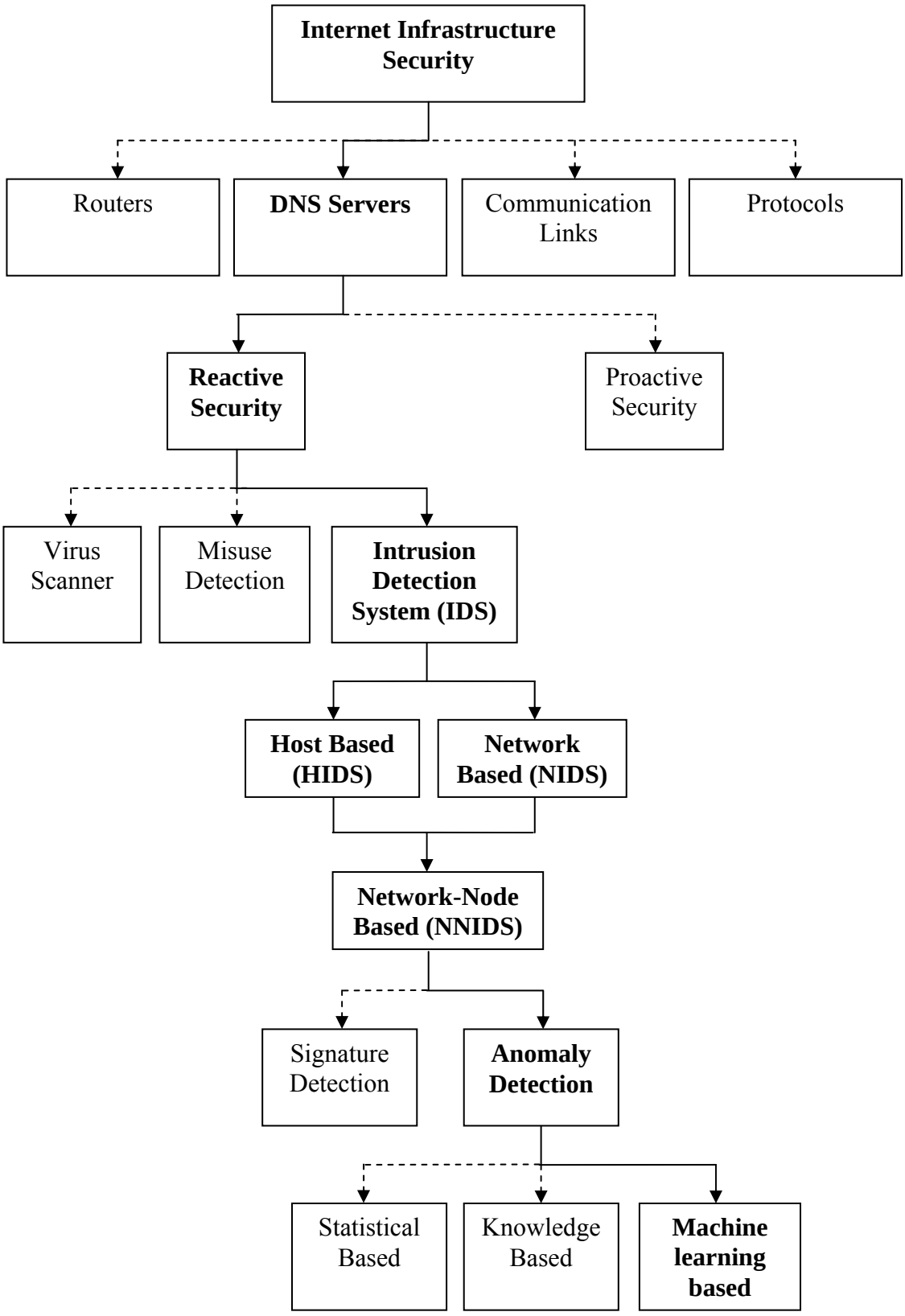

Figure 1. 1. Study module