BORANG PENGESAHAN STATUS TESIS*

JUDUL: Misuse Detection System using Artificial Neural Network__________
SESI PENGAJIAN: 2007/2008_
Saya AMIRAH NABIHAH BT JAHIDIN______________________________
(HURUF BESAR)

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

1. Tesis dan projek adalah hakmilik 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 membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. **Sila tandakan(/)

_______SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub didalam AKTA RAHSIA RASMI 1972)

________TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

____/___TIDAK TERHAD

____
(TANDATANGAN PENULIS)

Alamat tetap: Lot 1904, LRG B4,
RPR Fasa 2, Petra Jaya, 93050____
Kuching, Sarawak.__________

Tarikh: 2/5/08

____
(TANDTANGAN PENYELIA)

En. Nazrulazhar Bahaman__
Nama Penyelia

Tarikh: 2-5-08

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

MISUSE DETECTION SYSTEM USING ARTIFICIAL NEURAL NETWORK

AMIRAH NABIHAH BT JAHIDIN

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

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2008

DECLARATION

I hereby declare that this project report entitled

MISUSE DETECTION SYSTEM USING ARTIFICIAL NEURAL NETWORK

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : ______________________ Date: 2/5/08
(AMIRAH NABIHAH BT JAHIDIN)

SUPERVISOR : ______________________ Date: 2-5-08
(EN. NAZRULAZHAR BAHAMAN)

DEDICATION

Special dedicated to my beloved parents who have encouraged and inspired me throughout my journey of education. No forgotten, my lecturer and friends.

AKNOWLEDGEMENTS

I would like to take the chance to acknowledge the contributions of a number of people. I deeply appreciate their valuable contribution in my Projek Sarjana Muda program and the thesis project. I would like to begin my thanksgiving to my supervisor Encik Nazrulazhar Bahaman who had thought, guided me through this thesis project development, believe that I can do this project even I am not expose to the artificial intelligent is my studies. Thank you so much sir.

Also, I would like to express my sincere thank for all PSM committees, lecturer of faculty of Information Technology and Communication who really doing hard to give explanation and opinion about this thesis project. The project would not run smoothly without the guidance from them.

Last but not least, I send my special thanks to my parent, siblings and friends, for their undying support, thought and encouragement during study in Universiti Teknikal Malaysia Melaka.

Thank you so much everyone. May Allah bless you all.

ABSTRACT

The system developed for Projek Sarjana Muda (PSM) is entitled Misuse Detection System using Artificial Neural Network. It is a system that detects misuse based on packet with the help of neural network and using feedforward backpropagation technique. The system operates offline and use data from DARPA during training and testing. The system believes capable to identify network attacks by training the neural network to recognize data that contain normal packet against data that contain misuse packet that probably intent to attack the network. The project is targeted to deliver a system that able to identify normal and misuse packet. Most current approaches to misuse detection involve the use of rule-based expert systems to identify indications of known attacks. However, these techniques are less successful in identifying attacks which vary from expected patterns. Artificial neural networks provide the potential to identify and classify network activity based on limited, incomplete, and nonlinear data sources. This paper presents an approach to the process of misuse detection that utilizes the analytical strengths of neural networks which at the end of the project, Misuse Detection System using Artificial Neural Network is proved capable to detect misuse in network by identified misuse and normal packet that results with 98% accuracy.

ABSTRAK

Sistem yang dibangunkan untuk Projek Sarjana Muda ini dikenali sebagai Sistem Pengesan Penyalahgunaan Menggunakan Kecerdikan Rangkaian Neural. Sistem ini berfungsi mengesan penyalahgunaan di dalam rangkaian berdasarkan paket dengan bantuan kecerdikan rangkaian neural dan teknik 'feedforward backpropagation'. Sistem ini beroperasi secara tanpa wayar dan menggunakan data daripada DARPA semasa proses melatih dan menguji rangkaian neural. Sistem ini juga dipercayai mampu untuk mengenalpasti serangan keatas rangkaian dengan lebih tepat kerana ia telah melalui proses latihan menggunakan paket normal dan paket yang disalahguna yang selalunya dihantar melalui rangkaian bertujuan untuk menlumpuhkan rangkaian. Pada akhir projek, sistem dijangka dapat mengesan paket normal dan paket yang disalahguna dengan tepat. Kebanyakan pendekatan keatas pengesan penyalahgunaan melibatkan penggunaan sistem peraturan berasas yang cekap untuk mengenalpasti serangan yang telah diketahui. Tetapi, teknik ini kurang berkesan untuk mengenalpasti serangan yang datang daripada pelbagai jenis. Kecerdikan rangkaian neural mempunyai kebolehan untuk mengesan dan mengelaskan aktiviti rangkaian yang mempunyai data yang terhad, tidak lengkap dan tidak tersusun. Kertas kajian ini menunjukkan pendekatan kepada proses mengesan pengalahgunaan yang memperkukuhkan kebolehan rangkaian neural di mana pada akhir projek, Sistem Pengesan Penyalahgunaan Menggunakan Kecerdikan Rangkaian Neural ini terbukti berkemampuan untuk mengesan penyalahgunaan di dalam rangkaian apabila ia mampu mengenal paket normal dan paket yang disalahguna dengan ketepatan sebanyak 98%.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ANN	-	Artificial Neural Network
ASSN	-	Associative Neural Network
CoM	-	Committee of Machines
DARPA	-	Defense Advanced Research Projects Agency
DoD	-	Department of Defense
ESN	-	Echo State Network
FIFO	-	First In First Out
FTP	-	File Transfer Protocol
GUI	-	Graphical User Interface
IP	-	Internet Protocol
kNN	-	k-Nearest Neighbour
LAN	-	Local Area Network
MDS	-	Misuse Detection System
MLP	-	Multi Level Protocol
NSM	-	Network Security Monitor
PSM	-	Projek Sarjana Muda
RAD	-	Rapid Application Development
RBF	-	Radial Basis Function
RMS	-	Root Mean Square
RN	-	Recurrent Network
SNNS	-	Stuttgan Neural Network Simulator

SOM	-	Self-organizing Map
SRN	-	Simple Recurrent Network
WAN	-	Wide Area Network

LIST OF ATTACHMENTS

CHAPTER I

INTRODUCTION

1.1 Project Background

The sensible and precise detection of computer and network system intrusions has always been an intangible goal for system administrators and information security researchers. The individual creativity of attackers, the wide range of computer hardware and operating systems, and the ever changing nature of the overall threat to target systems have contributed to the difficulty in effectively identifying intrusions. While the complexities of host computers already made intrusion detection a difficult attempt, the increasing prevalence of distributed network-based systems and insecure networks such as the intemet has greatly increased the need for intrusion detection.

Intrusion detection techniques have been traditionally classified into one of two methodologies: anomaly detection or misuse detection. Anomaly detection identifies activities that vary from established patterns for users, or groups of users. Anomaly detection typically involves the creation of knowledge bases that contain the profiles of the monitored activities while misuse detection is considered complementary to anomaly detection. The rationale is that known attack patterns can be detected more effectively and efficiently by using explicit knowledge of them. Thus, misuse detection systems look for well-defined patterns of known attacks or vulnerabilities. They can catch an intrusive activity even if it is so negligible that the anomaly detection approaches tend to ignore it.

Example of current approaches to misuse detection system is the process of detecting intrusions. It utilizes some form of rule-based analysis. Rule-Based analysis relies on sets of predefined rules that are provided by an administrator, automatically created by the system, or both. Expert systems are the most common form of rule-based intrusion detection approaches. Unfortunately, expert systems require frequent updates to remain current. While expert systems offer an enhanced ability to review audit data, the required updates may be ignored or performed infrequently by the administrator. At a minimum, this leads to an expert system with reduced capabilities.

Unlike expert systems, which can provide the user with a definitive answer if the characteristics which are reviewed exactly match those which have been coded in the rule base, a neural network conducts an analysis of the information and provides a probability estimate that the data matches the characteristics which it has been trained to recognize. While the probability of a match determined by a neural network can be 100%, the accuracy of its decisions relies totally on the experience the system gains in analyzing examples of the stated problem.

A limited amount of research has been conducted on the application of neural networks to detecting computer intrusions. Only few have an eager to study and implement the neural network in identifying misuse detection. As the matter approach, this project on misuse detection system is to enhance the existing misuse detection system by training the neural network with more packets to achieve solution that can lead to accurate result of finding misused in network. This system is design to function offline as a first stage approach in using artificial neural network. The solution is trained using Matlab Neural Network Toolbox while the interface is created using Matlab

Graphical User Interface that will implement the frozen solution as the main engine of the system. The system is function by allowing user to input Excel file that contain eight packet data for misuse detection. After inputting the file, the misuse detection process will proceed by loading the network, maximum and minimum values into Matlab Workspace with a click of a button. Then, command that availablein file will that can be open by clicking a button is copy to the Matlab Command Window in order to complete the process of misuse detection. The output can be view by clicking button that function to display output which when the button is clicked, the output that saved in Excel file will be displayed. The system also provide user guide in how to use the system to effortless first time user in using it. This system that detects misuse based on packet is called Misuse Detection System using Artificial Neural Network as it takes the approach of neural network.

1.2 Problem Statements

The increased connectivity between computer systems has opened up many possibilities of attacks. Examples of intrusive attacks are: attempted break-in (unauthorized users try to gain access to the system, typically associated with a high rate of login failures), tempered executables (Trojan horses or viruses, associated with atypical CPU and I/O activity, frequency of executables rewritten), denial of service (other users are denied access to certain services, associated with atypical usage pattern of system resources), leakage (attacker tries to leak information (e.g. covert channel), associated with atypical use of system resources), masquerade attack (an intruder tries to masquerade as a legitimate user, associated with, for instance, abnormal login time, location, connection type, different types of processes executed), malicious use (Legitimate users exploit their privileges, such as inference, aggregation, penetration, associated with excessive protection violation, directories browsing). These numerous attacks have tried to be trouncing with various of intruder and misuse detection system. But still, it has not stopping the intruder and attacker from stopping their dim behavior. It is because the totally secure system is not yet found.

Because of the increasing dependence which companies and government agencies have on their computer networks the importance of protecting these systems from attack is critical. A single intrusion of a computer network can result in the loss or unauthorized utilization or modification of large amounts of data and cause users to question the reliability of all of the information on the network. There are numerous methods of responding to a network intrusion, but they all require the accurate and timely identification of the attack.

Rule-based systems suffer from an inability to detect attacks scenarios that may occur over an extended period of time. While the individual instances of suspicious activity may be detected by the system, they may not be reported if they appear to occur in isolation. Intrusion scenarios in which multiple attackers operate in concern are also difficult for these methods to detect because they do not focus on the state transitions in an attack, but instead concentrate on the occurrence of individual elements. Any division of an attack either over time or among several seemingly unrelated attackers is difficult for these methods to detect.