Ain Shams University

Faculty of Computer & Information Sciences

Implementation of Intelligent Techniques for Intrusion Detection Systems

A Thesis Submitted to
Department of Computer Science
In partial fulfillment of the requirements for
The degree of Master of Science

by

Sahar Selim Fouad
B.Sc. Computer & Information Sciences
(Computer Science Department)

Under Supervision of

Prof. Dr. Taymoor M. Nazmy
Professor in Computer Science department,
Vice Dean of Higher Studies and Researches,
Faculty of Computer & Information Sciences,
Ain Shams University

Prof. Dr. Mohamed Hashem
Professor in Information System department,
Vice Dean of Educational & Students' Affairs,
Faculty of Computer & Information Sciences,
Ain Shams University

Cairo 2011

Acknowledgements

*Praise is to **Allah** and gratitude is given where it is due most to **Allah**.*

*So with genuine humility, I acknowledge the aid of **Allah**.*

*My deepest gratitude and sincerest appreciation to **Prof. Dr. Mohamed Hashem Abdel-Aziz**, for his continuous encouragement and enlightening advice and helpful advices, that helped me throughout this work.*

*I feel greatly indebted to **Prof. Dr. Taymoor M. Nazmy** for his dynamic efforts, sincere guidance and continuous support without which this work would have never seen the light.*

*Finally, I cannot sufficiently express my gratitude to my family; **my parents, my sisters**, my dearest friend **Manal Mohsen** whose love, support, guidance, and encouragement through the years have thoroughly equipped me for life, and my son **Abdel Rahman**, who makes it all worthwhile.*

Abstract

With the rapid expansion of computer networks during the past decade, security has become a crucial issue for computer systems. New security failures are discovered everyday and there are a growing number of bad-intentioned people trying to take advantage of such failures. Intrusion detection is a critical process in network security. Intrusion Detection Systems (IDS) aim at protecting networks and computers from malicious network-based or host-based attacks.

Different soft-computing based methods have been proposed in recent years for the development of intrusion detection systems. Most current approaches to intrusion detection involve the use of rule-based expert systems to identify indications of known attacks. Artificial neural networks and decision trees provide the potential to identify and classify network activity.

Most of the previous systems have some deficiencies. Some drawbacks of previous Intrusion detection systems (IDSs) are that they are unable to detect new attacks that are never seen before. Most of these systems don't identify the attack type but only specify whether the given network data is normal or attack. One of the drawbacks of IDSs that are signature-based is that they can only detect known attacks while all new unknown attacks will go unnoticed until the system is updated to be able to detect them.

This thesis proposes a hybrid intelligent intrusion detection system to improve the detection rate for known and unknown attacks. The introduced system has the capability to learn fast, enhanced capability of detection of new unidentified attacks, and alarming the system administrator of these unseen before attacks. Unlike other systems that have one level of detection, the proposed system has three levels of detection. The first level is where the system classifies the network users to either normal or intruder. The second level is where system can identify four categories of intruders (DOS, Probe, R2L & U2R). The third level is the fine detection level, where the attack type can be identified.

The proposed model consists of multi-level based on hybrid neural network and decision tree. We examined different neural network and decision tree techniques. Each module in each level is implemented with the technique (Neural Network or Decision Tree) which gave best experimental results for this module.

From our experimental results with different network data, our model achieves correct classification rate of 93.64%, average detection rate about 98%; 99.8% for known attacks and 93.8% for new unknown attacks.

The advantages of the proposed system is its ***high Detection Rate***, ***scalability*** (if new attacks of specific class are added to the dataset we don't have to train all the modules but only the modules affected by the new attack), ***adaptive*** (attacks that are misclassified by the IDS as normal activities or given wrong attack type will be relabeled by the network administrator. Training module can be retrained at any point of time which makes its implementation adaptive to any new environment or any new attacks in the network), ***generalization ability*** (the proposed system outperforms previous IDSs in detecting both known and new attacks which combines the advantages of signature-based and anomaly-based IDS). Also every module can be trained on separate computer in parallel which provides less training time.

CONTENTS

LIST OF FIGURES

Page

LIST OF TABLES

Introduction

Security of network system is becoming increasingly important as more sensitive information is being stored and manipulated online. It is difficult to prevent attacks only by passive security policies, firewall, or other mechanisms. Intrusion Detection Systems (IDS) have thus become a critical technology to help protect these systems as an active way. An IDS can collect system and network activity data, and analyze those gathered information to determine whether there is an attack [1].

Along with the conventionally used security tools like firewalls, intrusion detection systems (IDS) are becoming of supreme significance. Intrusion Detections Systems (IDS) is a new path of security systems, which provides efficient approaches to secure computer networks. Artificial Intelligence approaches have been used enormously to produce a lot of IDS. Some of these approaches rely on Neural Network to provide the network with an efficient classifier to recognize and detect intrusions actions.

The main objective of this work is to design and develop security architecture (an intrusion detection and prevention system) for computer networks. This proposed system should be positioned at the network server to monitor all passing data packets and determine suspicious connections. Therefore, it can inform the system administrator with the suspicious attack type. Moreover, the proposed system is adaptive by allowing new attack types to be defined.

We build the model to improve the detection rate for known and unknown attacks. First, we train and test our hybrid model on the normal and the known intrusion data. Then we test our system for unknown attacks by introducing new types of attacks that are never seen by the training module.

1.1 What's Intrusion?

When a user of an information system takes an action that user was not legally allowed to take, it is called intrusion. The intruder may come from outside, or the intruder may be an insider, who exceeds his limited authority to take action. Whether or not the action is detrimental, it is of concern because it might be detrimental to the health of the system, or to the service provided by the system [2].

Intrusion detection involves determining that some entity, an intruder, has attempted to gain, or worse, has gained unauthorized access to the system. None of the automated detection approaches of which we are aware seeks to identify an intruder before that intruder initiates interaction with the system. Of course, system administrators routinely take actions to prevent intrusion. These can include requiring passwords to be submitted before a user can gain any access to the system, fixing known vulnerabilities that an intruder might try to exploit in order to gain unauthorized access, blocking some or all network access, as well as restricting physical access. Intrusion detection systems are used in addition to such preventative measures [2].

1.2 Firewall Evasion

Many people consider firewalls "the best solution for ensuring network security". However, although these solutions are rather efficient, they do not provide reliable protection against all types of attacks. Firewall system neither detects and nor locks attacks. A firewall is a device that at first prohibits everything, and then permits only those things that must be determined by the administrator. In other words, when the firewall is installed, all connections between the network being

protected and the external network are prohibited. After that, the administrator adds specific rules that enable specified traffic to pass through the firewall. A typical firewall configuration prohibits all incoming ICMP traffic, leaving only outgoing traffic enabled, along with some types of incoming traffic based on the UDP and TCP protocols (such as HTTP, DNS, SMTP, etc.). This configuration will allow employees to access the Internet and deny intruders access to internal resources of the network. Firewalls can not state for sure if an attack is present in the traffic. They can only inform the administrator whether or not the traffic satisfies the requirements established by the specific rules [3].

Firewalls prevent certain kinds of attacks, they protect communications between networks (typically internal network and the Internet), and offer no or little protection from attacks or misuse within local network. If network perimeter is breached, or if the misuse is internal to organization, a Firewall offers no help [3].

This fact is best explained by the following analogy. Consider the firewall to be a "fence" around your network, which simply limits access to specific points behind it, but can not detect if someone is trying to dig a tunnel under it [3].

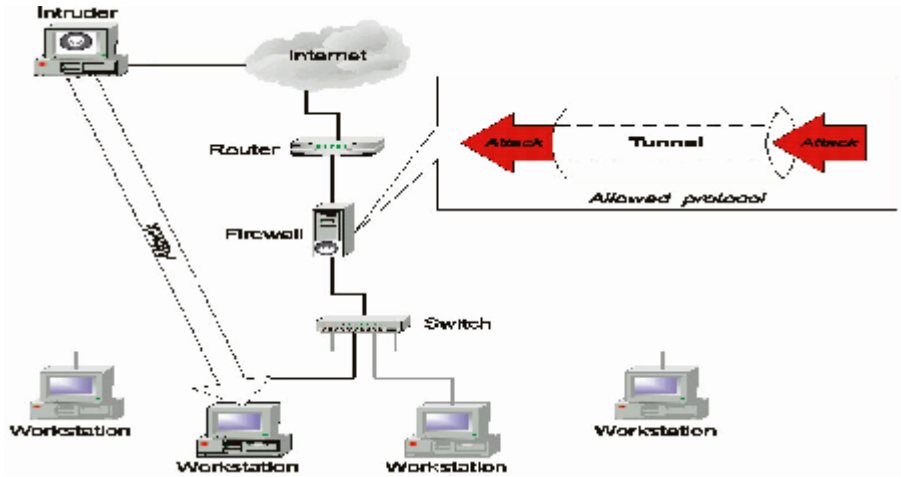

Figure 1.1 Attack via tunnels in a firewall

1.3 Classification of Intrusion Detection Systems

Intrusion detection systems attempt to detect attacks against computer systems and networks. Traditionally, intrusion detection systems can be classified using two approaches, namely, data source and detection approach [4].

1.3.1 Classification Based on Data Source

Based on the source of input data, an Intrusion Detection System (IDS) can be classified as follows [4]:

1. **Host-based IDS:** Deployed on a host computer, the IDS monitors only the activity of that particular host. Information such as operating system audit trails, registry entries and file accesses is used to detect an intrusion.

2. **Network-based IDS:** It resides on a separate system that watches network traffic, looking for indications of attacks that traverse that portion of the network. It passively monitors the network activities of a particular host or a network of hosts.

3. **Hybrid/Hierarchical IDS:** A Hybrid/Hierarchical IDS combines the advantages of host-based and network-based IDSs. Improved intrusion detection capability is achieved through analysis of both host and network data.

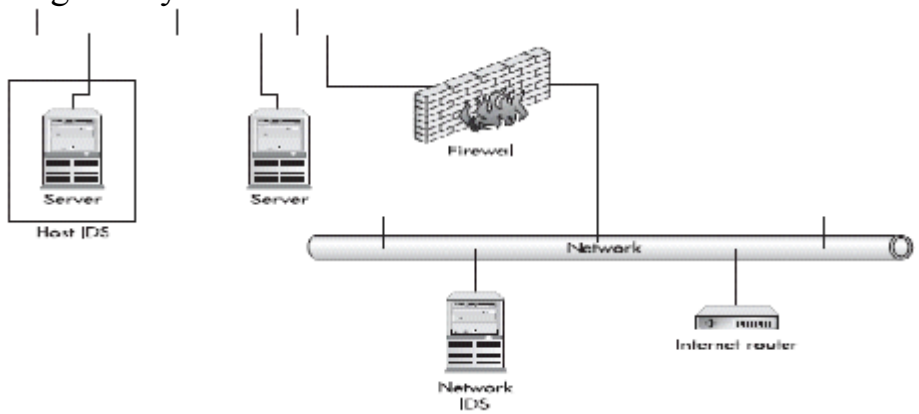

Figure 1.2 Shows how the two types of IDS may exist in a network environment.

The distinction is useful because network-based intrusion detection tools usually process completely different data sets and features than host-based intrusion detection. As a result, the types of attacks that are detected with network-based intrusion detection tools are usually different than host-based intrusion detection tools. Some attacks can be detected by both network-based and host-based IDSs, however, the "sweet spots", or the types of attacks each is best at detecting, are usually distinct. As a result, it is difficult to make direct comparisons between the performance of a network-based IDS and a host-based IDS. A useful corollary of distinct sweetspots, though, is that in combination both techniques are more powerful than either one by itself [5]. Table 1 shows some of the differences between a HIDS and a NIDS [6].

Table 1.1: Network-Based vs. Host-Based Intrusion-Detection Systems

HIDS	NIDS
Broad in scope (watches all network activities)	Narrow in scope (watches only specific host activities)
Easier setup	More complex setup
Better for detecting attacks from the outside	Better for detecting attacks from the inside
Less expensive to implement	More expensive to implement
Detection is based on what can be recorded on the entire network	Detection is based on what any single host can record
Examines packet headers	Does not see packet headers
Near real-time response	Usually only responds after a suspicious log entry has been made
OS-independent	OS-specific
Detects network attacks as payload is analyzed	Detects local attacks before they hit the network
Detects unsuccessful attack attempts	Verifies success or failure of attacks