Computer Science Department
Faculty of Computer & Information Sciences
Ain Shams University

DESIGN OF MULTI-AGENT BASED SYSTEM FOR APPLICATION BASED INTRUSION DETECTION

This thesis is submitted as a partial fulfillment of the requirements for the degree of Master of Science in Computer and Information Sciences.

By
Islam Mohamed ElSayed Hegazy
B.Sc. in Computer and Information Sciences,
Demonstrator at Computer Science Department,
Faculty of Computer and Information Sciences,
Ain Shams University.

Under Supervision of
Prof. Dr. Taha ElArif
Computer Science Department,
Prof. of Computer Science,
Faculty of Computer and Information Sciences,
Ain Shams University.

Prof. Dr. Mostafa Syiam
Head of Computer Science Department,
Vice dean for students' affairs,
Faculty of Computer and Information Sciences,
Ain Shams University.

Dr. Hossam M. Faheem
Computer Science Department,
Lecturer of Computer Science,
Faculty of Computer and Information Sciences,
Ain Shams University.

Cairo 2005

ACKNOWLEDGMENT

First, thanks to God, the most beneficent and the merciful.

I sincerely acknowledge and express my appreciation to *Prof. Dr. Mohamed Said Abd El Wahab*, the Dean of the faculty of Computer and Information Sciences, Ain shams University, for his support, valuable comments, concern and thankful help.

I would like to thank *Prof. Dr. Taha Al-Arif* and *Dr. Hossam Mostafa* for their continuous support, and useful supervision. Special thanks to *Prof. Dr. Mostafa Syiam and Prof. Dr. Essam Atta* for their careful evaluation of my work. I deeply indebted to them for giving this work the suitable final form.

Thanks also to Dr. Zaki Taha, Dr. Ashraf Saad, and my friends and colleagues Wael Othman, Mohamed Abd El-Megeed, Safia Abbass, Mohamed Marey, Salma Hamdy, Mohamed Samy, and Talal.

I cannot express my feelings towards my family who supported me all over through my way and backed me up during my studies wishing me good luck throughout the preparation of this thesis.

ABSTRACT

Network security demands have increased considerably during the last few years. One of the critical networking security applications is the intrusion detection system. Intrusion detection systems should be fast enough to catch different types of intrusions. Due to the arising of new attacks in the cyber world everyday new intrusion detection systems have to be built to cope with these new attacks. Intelligent agents are now used in several fields of computer science. They are ideally qualified to play an important role in intrusion detection systems due to their reactivity, interactivity, autonomy, and intelligence.

In this thesis, a framework for multiagent-based system for intrusion detection using the agent-based technology is designed and implemented. The proposed system is implemented over a multi-threaded program to demonstrate the framework. It is considered a step towards a complete multiagent-based system for network security.

The proposed system uses cooperating agents to perform the detection process for three types of attacks: secure document theft, denial of service attacks, and ping sweep attacks. It uses two detection methodologies: network-based intrusion detection and application-based intrusion detection. It may take an active response, disconnecting the intruder, or just alerting the system administrator.

A testing methodology for evaluating intrusion detection systems that clarifies methods and procedures to be carried out when testing intrusion detection systems is introduced. The performance of the proposed system is evaluated by conducting two groups of experiments according to this methodology. The system is tested against three evaluation factors: risk time, detection ratio, and the intrusion ratio. In the first group, the

system is dedicated to detect a single type of attacks. Whereas in the second group, the system detects all the types of attacks. The experimental results of the proposed system are compared to other research projects and have shown better detection ratios. Also, the characteristics of the proposed system are compared to the characteristics of other intrusion detection systems.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Overview

Security is one of the major issues for any network. It involves securing resources from damages and intruders. Making a network completely secure is practically impossible since there are a lot of areas to be protected and also new threats arise everyday. The solution to this problem is to try to build intelligent systems that are capable of securing the network and learn from their experience over time.

The Internet protocol was originally developed to connect a group of scientists who need to share scientific information. It was developed by the department of defense (DoD) of the United States. Then it began to gain popularity through ordinary people such that anyone can connect to the Internet with a small computer. Companies connecting their networks to the Internet found that they had to secure their resources and information from unauthorized access.

Computer security deals with prevention and detection of unauthorized actions by users of a computer system. For a secure system to be successful, there should be some protective measures; prevention: take measures that prevent your assets from being damaged. Detection: take measures that allow you to detect when an asset has been damaged, how it has been damaged, and who has caused the damage. Reaction: take measures that allow you to recover your assets or to recover from damage to your assets [1].

Also, a secured system has to cover three aspects; confidentiality: prevention of unauthorized disclosure of information. Integrity: prevention of unauthorized modification of information. Availability: prevention of unauthorized withholding of information or resources [1].

Generally, computer security has to keep unauthorized users from accessing sensitive information. The role of confidentiality is to maintain this feature. Another feature of computer security is to ensure that information is consistent and not corrupted (integrity). Also, computer security should make sure that the authorized users could access the information they are authorized to use and that is maintained by the availability aspect.

An agent is an autonomous computational entity such as a software program that can be viewed as perceiving and acting upon its environment and that is autonomous in that its behavior at least partially depends on its experience. It operates flexibly and rationally in a variety of environmental circumstances given its perceptual and effectual equipment. An agent on the basis of key processes such as problem solving, planning, decision-making, and learning achieves behavioral flexibility and rationality. As an interacting entity, an agent can be affected in its activities by other agents and perhaps by humans. A key pattern of interaction in multiagent systems is goal- and task-oriented coordination, both in cooperative and in competitive situations. In the case of cooperation several agents try to combine their efforts to accomplish as a group what the individuals cannot, and in the case of competition several agents try to get what only some of them can have. The long-term goal is to develop mechanisms and methods that enable agents to interact as well as humans, and to understand interaction among intelligent entities whether they are computational, human, or both [2].

What makes an intelligent agent different from a typical computational procedure is the fact that intelligent agents posses among other characteristics, the ability to satisfy their goals, based upon their former interaction with other agents [3].

Multiagent system is a software system that consists of multiple agents that communicate and cooperate with each other to solve complex problems and implement complex systems [4].

1.2 Motivations

Rapid development realms of artificial intelligence (A.I.) could have been more efficiently utilized keeping in mind that intelligent agents are gaining more attention in developing security tools due to its intrinsic features.

We have two main reasons to build an intrusion detection system with agents. The first reason is that multiagent systems have the capacity to play a key role in current and future computer science and its application. Modern computing platforms and information environments are distributed, large, open, and heterogeneous. The increasing complexity of computer and information systems goes together with an increasing complexity of their applications. These often exceeds the level of conventional, centralized computing because they require the processing of huge amounts of data, or of data that arises at geographically distinct locations. To cope with such applications, computers have to act more as agents, rather than just parts.

The second reason is that multiagent systems have the capacity to play an important role in developing and analyzing models and theories of interactivity in human societies.

Humans interact in various ways and at many levels: for instance, they observe and model, they request and provide information, they negotiate and discuss, they develop shared views of their environment, they detect and resolve conflicts, and they form and dissolve organizational structures such as teams, committees, and economics.

1.3 Objectives

The objective of this thesis is to build an intrusion detection system using software agents. The intrusion detection system should be able to detect, analyze, and deny access to intruders in an acceptable time interval such that the multiagent-based system will be ideally qualified to protect networks subject to attacks in real time.

1.4 Thesis outline

The thesis is organized as follows: chapter 2 discusses network security issues regarding types of threats, kinds of attacks, points of weaknesses, and security controls. Chapter 3 provides background information about the different techniques of implementing intrusion detection systems, the anatomy and characteristics of intrusion detection systems. Also, it discusses the types of agents, their environments, and their applications. Chapter 4 explains the proposed framework for building an intrusion detection system, and highlights the use of agents in this framework. Chapter 5 highlights the performance of the system by explaining the groups of the experiments conducted on the proposed system and their results. Also, it provides the comparisons conducted with other research projects regarding the experimental results and the characteristics. Finally, the conclusion of the thesis and the suggested future work.

Chapter 2

Network Security

2.1 Introduction

External network attacks can be categorized into IP spoofing attacks, packet sniffing, sequence number predication attacks and trust-access attacks. Categories of internal attacks include passwords attacks, session hijacking attacks, shared library attacks, and technological vulnerability attacks [5].

Computer network security can be categorized as follows [5]:

1. Security enhancement software: thus replacing an operating system's built-in security software.
2. Authentication and encryption software: encrypts and decrypts computer files.
3. Security monitoring software monitor: monitors different operations of a computer network and outputs the results to system administrators.
4. Network monitoring software: monitors user's behavior or monitors incoming and outgoing traffic.
5. Firewall software and hardware: runs on the Internet/intranet entrance to a computer network, and checks all incoming network traffic for its contents at the network and transport layers of the OSI model.

2.2 Types of threats

There are various types of threats that attack networks. These attacks are summarized in eavesdropping, masquerade, replay, data manipulation, misrouting, trapdoor, viruses,