IGI PUBLISHING **ITB14883**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-pub.com

This paper appears in the publication, **Web Services Security and E-Business**
edited by **G. Radhaman & G. S. V. Radha Krishna Rao**

Chapter XIII

Distributed Intrusion Detection Systems: An Overview

Rosalind Deena Kumari, Multimedia University, Malaysia

G. Radhamani, Multimedia University, Malaysia

Abstract

The recent tremendous increase in the malicious usage of the network has made it necessary that an IDS should encapsulate the entire network rather than at a system. This was the inspiration for the birth of a distributed intrusion detection system (DIDS). Different configurations of DIDSs have been actively used and are also rapidly evolving due to the changes in the types of threats. This chapter will give the readers an overview of DIDS and the system architecture. It also highlights on the various agents that are involved in DIDS and the benefits of the system. Finally, directions for future research work are discussed.

Introduction

Intrusion detection (ID) is a term that is used for an automated security system that can identify attempts made to violate security of the system. The main objective of this system is to detect unusual activity such as a large number of unsuccessful login

attempts from one point or several attempts made to access the password of a file. The method is based on statistical analysis or rule-based expert systems. Intrusion detection is a powerful security tool because of its ability to counter attacks from insiders who misuse their privileges, and attacks resulting from such events as lost or stolen passwords or cryptographic keys.

Different ID systems have differing classifications of "intrusions"; a system attempting to detect attacks against Web servers might consider only malicious HTTP requests, while a system intended to monitor dynamic routing protocols might only consider RIP spoofing (Ford, 1994). A security system cannot be complete without intrusion detection and an ID system complements other security technologies. The ID system provides information to the site administration regarding detection of attacks that are handled by other systems, as well as about new attacks unforeseen by other security components. It also provides information that is useful to track the origin of the attack. This helps in restricting attackers, as their identity would be revealed. But an IDS is limited to individual machines, which does not secure an entire network of machines.

Intrusion detection approaches can be divided into two categories:

- **Anomaly detection model:** Anomaly detection uses the method of modeling normal behavior. Any instances of violation of this model are considered to be of concern and suspicious. For example, a normally inactive public Web server attempting to open connections to a large number of addresses may be indication of a worm infection.
- **Misuse detection model:** Misuse detection tends to model abnormal behavior, any occurrence of such behavior clearly indicates system abuse. For example, an HTTP request referring to the cmd.exe file may indicate an attack.

Anomaly detection is bugged from accuracy problems, whereas misuse detection can reach high levels of accuracy. The major problem in misuse detection is creation of compact models of attacks. Since these two methods are complementary in nature, many systems tend to combine both of these techniques (Du, Wang, & Pang, 2004)

A DIDS consists of multiple intrusion detection systems (IDS) covering a large network, and all the IDSs communicate with each other, or with a central server that provides advanced network monitoring, incident analysis, and instant attack data. As these cooperative agents are distributed across a network, incident analysts, network operations personnel, and security personnel will be able to get a broader view of the occurrences on their network as a whole. A DIDS enables a company to efficiently manage its incident analysis resources with a centralized database of its attack records, and by giving the analyst a quick and easy way to identify new trends and patterns and to pinpoint threats on the network across multiple network segments (Zhang, Xiong, & Wang, 2005).