IGI PUBLISHING **ITB14877**

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 VII

Intrusion Detection System: A Brief Study

Robin Salim, Multimedia University, Malaysia

G. S. V. Radha Krishna Rao, Multimedia University, Malaysia

Abstract

This chapter introduces the intrusion detection system (IDS). It starts with a brief explanation of the history of IDS and proceeds with generic components of IDS. Besides highlighting current advances in IDS, the chapter describes recent challenges to the system. The authors hope that this chapter sheds a light for readers who are unfamiliar with this domain.

Introduction to Intrusion Detection System

Intrusion detection is the process of monitoring events occurring in a computer system or network and analyzing them for signs of security problems. The intrusion detection system itself is a system to realize such a process. Early work on the IDS involves military and governmental agencies. Among the reasons was that an increasing number of agencies were using computers for daily operations. Hence, it was deemed necessary to assure the system was secured.

In the realm of information technology, IDS works by observing a computer system for any sign of intrusion through anomalous event or misuse signature. The primary goal of IDS is detecting any security breaches, preferably in real time. The intrusion detection system is an important security tool that complements various computer security products. It acts as the burglar alarm for information systems, ringing alerts and sending notifications on the occurrence of a computer security incident. Not to be confused with a prevention system, IDS does not in anyway modify the current environment setting besides alerting the responsible party.

Many times information security is related to confidentiality, availability, and integrity of information. From this perspective, one can infer that intrusions are the act that breaches any of confidentiality, availability, and integrity. The intrusion detection goal is to detect those incidents. By detecting them in time, appropriate actions can be taken either by the security officer or handled by the system itself.

As it advances, the computer system domain has become more sophisticated. In order to fulfill infinite human needs, the computer has become faster, processing more data, and as a result has become more complex. With that in mind, in order to detect attacks, IDS faces even greater challenges. In order to deliver response in near real time, the observer must perform faster than the object being observed. There are more applications and services deployed. In order to meet real-life scenarios, more network protocols have been deployed. As a result, the attack vector has increased. In order to recognize attacks, IDS needs to understand the object being monitored. For example, in network-based IDS, deep-packet inspection could help in analyzing network attacks.

The intrusion prevention system (IPS) is the logical evolution of IDS. Besides sending alerts, it also tries to prevent further damages. For instance, it reconfigures the firewall automatically, modifies the access control list (ACL) at network gateway to block suspicious conversation or even reroute a suspicious packet through. By saying that, we are actually witnessing the combination of functions from various networking nodes. Besides that, in order to support its task, there needs to be communication among IDS in the network.

History and Background of Intrusion Detection

During the 1980s, computer systems had already been equipped with audit capability. With such a component, the operating system could gather system-wide attributes. As events gathered were increasing, and analysis being done by humans was tedious, there needed to be an automated method of correlating audit data to produce important information. This automated tool was the root of IDS. IDS originates from the information audit field.

Among the first IDS was Denning and Neumann's intrusion detection expert system (IDES) (Denning, 1986). The research, funded under the U.S. Navy's Space and Naval Warfare, proposed the use of profiles in monitoring subjects of interest. It used statistical