Fuzzy Intrusion Detection System

Piyakul Tillapart, Thanachai Thumthawatworn and Pratit Santiprabhob
Faculty of Science and Technology, Assumption University
Bangkok, Thailand

Abstract

A framework for intrusion detection system (IDS) over TCP/IP network is proposed. The key idea is to use soft computing for detecting intrusive behaviors and Denial of Service attacks (DoS). The basic intent of a DoS attack either overwhelms the resources allocated by a networked device to a particular service in order to prevent its use or crashes a target device or system. This will cause disaster in network environment. To protect the most valuable possession from these malicious attempts is so essential. Fuzzy rule-based system has been introduced to implement IDS in this framework. The experimental results reveal that the proposed framework yields better result of detection than traditional threshold-based detection.

Keywords: *Intrusion detection system, fuzzy rule-based system.*

Introduction

Network grows very fast in its size and many networks are tied together to form the inter-network, then the network resources become the most valuable possession for all the organizations. Consequently these network resources become the targets for both the investors and attackers. The system penetrations that come from both inside and outside the network are very terrible. There are not only organizations' web servers that were attacked by the hackers but also other servers which provide services to the customers or subscribers; they were compromised by the intruders. Therefore, these organizations could not provide services for some moment of time (Lee 2000).

To protect these network resources from the intruders, the intrusion detection systems (IDSs) have been developed (Lunt *et al.* 1989; Lunt *et al.* 1992; Rice 2001; Snapp *et al.* 1991). The IDS is used for detecting the intrusions that are defined to be unauthorized uses, misuses, or abuse of computer system by authorized users or external perpetrator. These systems are divided into host-based IDSs and network-based IDSs. Host-based IDSs are used to secure critical network servers of other systems containing sensitive information, while network-based IDSs monitor activity on a specific network segment. These IDSs have been proposed using different methods for detecting intrusions.

This paper proposes the framework for real-time fuzzy intrusion detection system (FIDS) that is able to detect and suspect the DoSs by employing fuzzy rule-based system (Earl 1994), and to provide useful information that can help the system administrator (SA) to take action against them. The input traffic has been captured from the operating network. This input traffic contains both normal and abnormal traffic. The input data must be preprocessed before sending to FIDS detector. The results obtained from the experiment reveal that the proposed framework works well when the networks have either low rate or high rate of intrusion. The unnecessary warning messages will not be generated. This allows the SA to take the appropriate actions to such attacks.

The Purposed Framework

This section discusses the architecture of the proposed framework for FIDS. It addresses to detect several kinds of attacks: syn-flood attack, udp-flood attack, ping-of-death attack, e-mail bomb, FTP and telnet password guessing, and port scanning. The framework uses fuzzy rule-based system to detect the intrusive traffics and to alter the SA about these attacks. FIDS framework is shown in Fig. 1.