Chapter 6

USING MIB II VARIABLES FOR NETWORK INTRUSION DETECTION

Xinzhou Qin  
College of Computing  
Georgia Institute of Technology  
801 Atlantic Drive  
Atlanta, GA 30332 USA  
xinzhou@cc.gatech.edu

Wenke Lee  
College of Computing  
Georgia Institute of Technology  
801 Atlantic Drive  
Atlanta, GA 30332 USA  
wenke@cc.gatech.edu

Lundy Lewis  
Aprisma Management Technologies  
121 Technology Drive  
Durham, NH 03824 USA  
lewis@aprisma.com

João B. D. Cabrera  
Scientific Systems Company  
500 West Cummings Park, Suite 3000  
Woburn, MA 01801 USA  
cabrera@ssci.com

D. Barbará et al. (eds.), Applications of Data Mining in Computer Security  
Abstract

Detecting and resolving security and performance problems in distributed systems have become increasingly important and challenging because of the tremendous growth in network-based services. Intrusion detection is an important security technique for networks and systems. In this paper, we propose a methodology for utilizing MIB II objects for network intrusion detection. We establish the normal profiles of network activities based on the information provided by the MIB II variables and use data mining techniques and information-theoretic measures to build an intrusion detection model. We test our MIB II-based intrusion detection model with several Denial of Service (DoS) and probing attacks. The results have shown that the model can detect these attacks effectively.

Keywords: Intrusion Detection, Anomaly Detection, Data Mining, MIB II, Network Security Management

1. Introduction

An intrusion detection system (IDS) is an important component of network security mechanisms. An IDS collects audit data from the system and network activities, e.g., BSM [24] and tcpdump [12], and analyzes the information if there is an occurrence of intrusion or not.

There are two major intrusion detection techniques, i.e., misuse detection and anomaly detection. Misuse detection is a signature-based technique that identifies attacks based on the patterns of intrusion behavior or effects. Anomaly detection uses the established normal profiles to identify any unacceptable deviation as the possible result of an intrusion such as [16]. Anomaly detection is intended to detect new attacks that have no known signatures yet. Misuse detection cannot catch new intrusions, however, misuse detection can be more accurate and efficient than anomaly detection.

Building a good anomaly detection model is very difficult. Anomaly detection technique is based on the understanding of the normal activities of systems and networks. However, it is difficult to construct comprehensive profiles that cover all normal activities. Another difficulty in anomaly detection is the feature construction process. Generally, when building an IDS, we need to determine the features in order to effectively represent the network and system activities. Some of the features can be extracted from audit data directly, while others need statistics computed by using the audit data, for example, the number of incoming TCP segments within a certain period of time. It is nontrivial to decide what features should be extracted or computed.