Chapter 17
Advanced Security Incident Analysis with Sensor Correlation

Ciza Thomas  
College of Engineering, India

N. Balakrishnan  
Indian Institute of Science, India

ABSTRACT

This chapter explores the general problem of the poorly detected attacks with Intrusion Detection Systems. The poorly detected attacks reveal the fact that they are characterized by features that do not discriminate them much. The poor performance of the detectors has been improved by discriminative training of anomaly detectors and incorporating additional rules into the misuse detector. This chapter proposes a new approach of machine learning method where corresponding learning problem is characterized by a number of features. This chapter discusses the improved performance of multiple Intrusion Detection Systems using Data-dependent Decision fusion. The Data-dependent Decision fusion approach gathers an in-depth understanding about the input traffic and also the behavior of the individual Intrusion Detection Systems by means of a neural network learner unit. This information is used to fine-tune the fusion unit since the fusion depends on the input feature vector. Thus fusion implements a function that is local to each region in the feature space. It is well-known that the effectiveness of sensor fusion improves when the individual IDSs are uncorrelated. The training methodology adopted in this work takes note of this fact. For illustrative purposes, the DARPA 1999 data set as has been used. The Data-dependent Decision fusion shows a significantly better performance with respect to the performance of individual Intrusion Detection Systems.

INTRODUCTION

The threat of attacks on the Internet is quite real and frequent and this has led to an increased need for securing any network on the Internet. An Intrusion Detection System (IDS) provides an additional layer of security to network’s perimeter defense, which is usually implemented using a firewall. The goal of an IDS is to collect information from a variety of systems and network sources, and then analyze the information for signs of intrusion and misuse. IDSs are implemented in hardware, software, or a combination of both.
The network traffic is made up of attack or anomalous traffic, and normal traffic. The real-world traffic is predominantly made up of normal traffic rather than attack traffic. Even in the attack traffic, some attacks are rarer. Rarer attacks may also cause significant damage. The IDSs are normally characterized by the overall accuracy. Though an IDS can give very high overall accuracy, its performance for the class of rarer attacks has been found to be less than acceptable as illustrated in the next section. Basic domain knowledge about network intrusions makes us understand that User to Remote (U2R) and Remote to Local (R2L) attacks are intrinsically rare. The problem of designing IDSs to work effectively and yield higher accuracies for minority attacks like R2L and U2R even in the mix of data skewness has been receiving serious attention in recent times.

The imbalance in data degrades the prediction accuracy. In most of the available literature this is overcome by resampling the training distribution. The resampling is done either by oversampling of the minority class or by undersampling of the majority class (Breiman, Friedman, & Olshen, 1984, Kubat, Holte, & Matwin, 1997, Chawla, Bowyer, Hall, & Kegelmeyer, 2002). The other commonly used approaches for overcoming data imbalance include the cost-sensitive learning (McCarthy, Zabar, & Weiss, 2005, Chan, & Stolfo, 1998), the two-phase rule induction method (Joshi, Agarwal, & Kumar, 2001), and rule based classification algorithms like RIPPER (Cohen, 1995) and C4.5 rules (Quinlan, 1993). However, none of these attempts have shown any significant contribution in overcoming the data skewness problems. Hence, in spite of all the earlier attempts, there is still room for a significant improvement in the detection of rare attacks.

There is an increased demand for effective monitoring of information systems. The importance of network situational awareness by developing engineering solutions and research approaches for analyzing broad network activity is beyond doubt. Since there is no perfect Intrusion Detection Systems (IDS), it is only natural to combine IDSs such that the weakness of one is compensated by the strength of another. Sensor fusion refers to a process that integrates and correlates heterogeneous data. It is the process of combining information from various suboptimal sources in order to obtain a more accurate and optimal result. The utility of sensor fusion for improved sensitivity and reduced false alarm rate of intrusion detection has been demonstrated in the literature (Bass, 1999). In view of enormous computing power available in present day processors, the trend to deploy multiple IDSs in the same network to obtain best-of-breed solutions has been attempted for enhancing the performance of attack detection. The goal of this chapter is to quantitatively detect threats and targeted intruder activity using a fusion architecture taking into account the correlation of the individual detectors. This chapter presents a method of combining the decisions of multiple IDSs using Data-dependent Decision fusion (DD fusion) technique. For illustrative purposes the DARPA 1999 dataset has been used. The performance of the data-dependent decision fusion IDS has been shown to be better than those reported so far for the minority attacks along with the improved performance for the majority attacks.

This chapter is organized as follows. The limitation of single IDSs and the need for sensor fusion is initially exemplified. This is done with reference to the DARPA dataset and with three IDSs, namely, Snort, Packet Header Anomaly Detector (PHAD), and Application Layer Anomaly Detector (ALAD). The chapter reviews the existing approaches followed by the discussion on the motivation behind the present study and the details of the presented approach. The data-dependent decision fusion architecture has been discussed. The chapter covers the implementation, discussion of the results and also the support proof for the use of DARPA dataset for IDS evaluation. The conclusion of the chapter is finally drawn after a discussion on the findings of this study.