Chapter 12
False Alarm Reduction: A Profiling Mechanism and New Research Directions

Salima Hacini
Constantine 2 University, Algeria

Zahia Guessoum
Pierre et Marie Curie University, France

Mohamed Cheikh
Constantine 2 University, Algeria

ABSTRACT

Intrusion detection systems (IDSs) are commonly used to detect attacks on computer networks. These tools analyze incoming and outgoing traffic for suspicious anomalies or activities. Unfortunately, these generate a significant amount of noise complexifying greatly the analysis of the data. This chapter addresses the problem of false alarms in IDSs. Its first purpose is to improve their accuracy by detecting real attacks and by reducing the number of unnecessary alerts. To do so, this intrusion detection mechanism enhances the accuracy of anomaly intrusion detection systems using a set of agents to ensure the detection and the adaptation of normal profile to support the legitimate changes that occur over time and are the cause of many false alarms. Besides this, as a perspective of this work, this chapter opens up new research directions by listing the different requirements of an IDS and proposing solutions to achieve them.

INTRODUCTION

Intrusion Detection Systems (IDSs) are essential complements to the preventive security mechanisms provided for computing systems and networks. They are used in the monitoring control process for the detection of potential intrusions and infections (Zanero, 2004).

DOI: 10.4018/978-1-5225-5583-4.ch012
The IDS research community has developed two categories of solutions: misuse detection and anomaly detection (Axelsson, 2000). The misuse detection defines, in a specific way, the user actions which constitute an abuse. Rules are therefore deduced for the detection of known intrusions. These rules are thus effective at detecting known intrusion attempts. However, they fail to recognize novel attacks (Wang, 2004). Anomaly detection (sometimes referred to as behaviour based) overcomes this limitation of misuse detection by focusing on normal behaviour, rather than attacks. For example, a heuristic analysis enables the generation of an alarm when the number of sessions bound for a given port exceeds a threshold in a preset time interval. This technique can be applied to both human users and software applications or services.

In spite of the noticeable development based on the anomaly techniques, the problem of the high rate of false alarms remains an open issue (Pokrywka, 2008; Khosravifar & Bentahar, 2008; Ohta et al., 2008; Jyothsna et al., 2011; Shruti et al., 2012). False alarms are indeed the main cause of alarm overload. Many recent researches report that false alarms still represent a consequent subset of the overall number of alarms (Nadiammai et al., 2011; Singh & Gupta, 2012) and several works have shown that the inspection of thousands of alarms per day is infeasible, especially if 99% of them are false positives (Perdisci et al., 2006). In fact, false alarms and timely identification of new attacks are among the biggest challenges to the effective use of IDSs. Thus, the success of anomaly detection systems relies on the development of detection approaches that improve the detection of attacks without misclassifying legitimate behaviour.

The implementation of anomaly-based detection systems requires the setting up of two phases: the training phase which allows the build of normal profile and the detection phase which enables the detection of all the activities that are out of the so-built normal profile. However, it is not possible to observe, during the training phase, all potential legitimate behaviours and the IDSs have to deal with dynamic changes and evolution of legitimate behaviour to adapt their diagnosis. So, based on the fact that Anomaly intrusion detection is used to find unknown attacks by using the concept of profiling normal behaviors and that significant false alarm may be caused because it is difficult to obtain complete normal behaviors (Jyothsna, Rama Prasad & Munivara Prasad, 2011), the normal profile must be adaptive. To do so, this chapter introduces a new Agent-based Adaptive Intrusion Detection mechanism (named AIDA). The latter relies on adaptation of the normal profile during the detection stage to minimize the number of false alarms and thus, enhances the accuracy of anomaly Intrusion Detection.

Moreover, to reduce the complexity of the current attacks, the proposed approach distributes their detection on a set of entities which cooperate to effectively detect the attacks and to adapt the normal profile when new legitimate activities appear. These entities are designed and implemented by agents; agents are the most suitable solution to the resolution of the problem of network intrusion detection (Boudaoud, 2000; Kannadiga & Zulkernine, 2005; Khosravifar & Bentahar, 2008; Zubair, 2012).

The proposed mechanism is used to study the network traffic and the malformed packets detection. The remainder of this chapter is organized as follows. Section 2 provides some work related to the problem of false alarms in intrusion detection. Section 3 gives an overview of AIDA and presents the associated agent-based architecture. Section 4 describes the adaptation process provided by AIDA. Section 5 defines the roles of the participating entities. Section 6 illustrates, through an example, the influence of the adaptation on the rate of false alarms. Section 7 is conducting a study on the required properties for a good IDS, the origins of errors generating false positives or false negatives and proposes research directions that could make improvements by providing it with these properties. Finally, Section 8 concludes the chapter.