Chapter 3.17
Adaptive Ensemble Multi-Agent Based Intrusion Detection Model

Tarek Helmy*
King Fahd University of Petroleum and Minerals, Saudi Arabia

ABSTRACT

The system that monitors the events occurring in a computer system or a network and analyzes the events for sign of intrusions is known as intrusion detection system. The performance of the intrusion detection system can be improved by combing anomaly and misuse analysis. This chapter proposes an ensemble multi-agent-based intrusion detection model. The proposed model combines anomaly, misuse, and host-based detection analysis. The agents in the proposed model use rules to check for intrusions, and adopt machine learning algorithms to recognize unknown actions, to update or create new rules automatically. Each agent in the proposed model encapsulates a specific classification technique, and gives its belief about any packet event in the network. These agents collaborate to determine the decision about any event, have the ability to generalize, and to detect novel attacks. Empirical results indicate that the proposed model is efficient, and outperforms other intrusion detection models.

DOI: 10.4018/978-1-60960-818-7.ch3.17

1. INTRODUCTION

Heavy reliance on the Internet has greatly increased the potential damage that can be inflicted by remote attacks launched over the Internet. It is difficult to prevent such attacks by security policies, firewalls, or other mechanisms. The computer system and the applications always contain unknown weaknesses or bugs attackers continually exploit them. Intrusion Detection Systems (IDS) are designed to detect attacks, which

Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

inevitably occur despite security precautions. A powerful IDS is flexible enough to detect novel attacks (i.e. it has the ability to generalize). The accuracy of the IDS depends on the false positive rate and the false negative rate measuring criteria. False positive rate calculates the rate of events that are considered to be intrusions where they are in fact normal events. However, false negative rate measures the rate of intrusions that are considered to be normal where they are in fact intrusion events.

Signature based Intrusion Detection (SID) uses specific known patterns of suspicious behavior to detect subsequent similar patterns, such patterns are called signatures. A good example for SID is a signature that can be as simple as a specific pattern that matches a portion of a network packet. For instance, packet header content signatures can indicate unauthorized actions. Once an intrusion action is detected, it triggers an alert or takes the initiative to do the proper action against the source of the attack (i.e. forward the traffic back to its source). The main disadvantage of this type of detection is that it cannot detect new signature attacks. It suffers also from the problem of signature updating. Snort is a well known example of SID (Roesch, 1999) on the other hand, Anomaly based Intrusion Detection (AID) identifies the normal usage behavior in advance and anything that does not match such behavior will be considered as suspicious actions. AID has the ability to generalize and to detect novel anomalies but cannot determine if the anomaly is caused by intrusive behavior or not. Hence, it generates higher false rate. USAID is an example of AID (Zhuowei et. al., 2005).

Several machine learning paradigms including Neural Networks (NN) (Mukkamala et. al., 2003), Linear Genetic Programming (LGP) (Mukkamala et. al., 2004), Support Vector Machines (SVM) (Mukkamala et. al., 2004), Bayesian Networks (BN) (Feng et. al., 2009), Multivariate Adaptive Regression Splines (MARS) (Mukkamala et. al., 2004), Decision Tree (DT) (Sandhya et. al., 2007), and Fuzzy Inference Systems (FISs) (Shah et. al., 2004) have been investigated for the design of the IDS.

The adaptivety of the IDS is a powerful feature that can lead the system to generalize and to detect novel attacks. By doing so, detection rate will increase, and the user's intension will be minimized. In this chapter, we propose an adaptive ensemble multi-agent-based intrusion detection model. In the proposed model, several agents are used in which each will encapsulate a classification algorithm. Based on the combined results generated from those agents, it is going to be decided whether a specific event in a network is an intrusion or not. The agent will also decide when to make a progress towards the adaptation. The rest of this chapter is organized as follows: Section 2 gives a brief overview of the related work. Section 3 elucidates the overview of the proposed framework architecture and specification. Section 4 describes the experimental dataset. The details of the implementation, the experimental results, and the performance comparison with other models are presented in Section 5. Finally, the conclusion and future work directions are outlined in Section 6.

2. RELATED WORK

A review of many alternative approaches to Intrusion Detection (ID) is available in (Bishop et. al., 1997). The most common approach to ID, often called "signature verification," detects previously seen, known, attacks by looking for an invariant signature left by these attacks. This signature may be found either in host-based audit records on a victim machine or in the stream of the network packets sent to a victim and captured by a "sniffer" which stores all important packets for on-line or future examination. The Network Security Monitor (NSM) was an early SID system that found attacks by searching for keywords in network traffic captured using a sniffer. Early versions of

11 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/adaptive-ensemble-multi-agent-based/56167

Related Content

A Generic Framework for Feature Representations in Image Categorization Tasks
Adam Csapo, Barna Resko, Morten Lind, Peter Baranyiand Domonkos Tikk (2012). *Software and Intelligent Sciences: New Transdisciplinary Findings (pp. 491-512).*
www.irma-international.org/chapter/generic-framework-feature-representations-image/65147

Adaptive Computation Paradigm in Knowledge Representation: Traditional and Emerging Applications
Marina L. Gavrilova (2009). *International Journal of Software Science and Computational Intelligence (pp. 87-99).*
www.irma-international.org/article/adaptive-computation-paradigm-knowledge-representation/2787

Inconsistency-Induced Learning for Perpetual Learners
Du Zhangand Meiliu Lu (2011). *International Journal of Software Science and Computational Intelligence (pp. 33-51).*
www.irma-international.org/article/inconsistency-induced-learning-perpetual-learners/64178

A Formal Knowledge Representation System (FKRS) for the Intelligent Knowledge Base of a Cognitive Learning Engine
Yousheng Tian, Yingxu Wang, Marina L. Gavrilovaand Guenther Ruhe (2011). *International Journal of Software Science and Computational Intelligence (pp. 1-17).*
www.irma-international.org/article/formal-knowledge-representation-system-fkrs/64176

An Artificial Intelligence-Based Vehicular System Simulator
Marvin T. Chan, Jonathan T. Chan, Christine Chanand Craig Gelowitz (2017). *International Journal of Software Science and Computational Intelligence (pp. 55-68).*
www.irma-international.org/article/an-artificial-intelligence-based-vehicular-system-simulator/175655