A New Negative Selection Algorithm for Adaptive Network Intrusion Detection System

Chikh Ramdane, Sétif 1 University, Sétif, Algeria
Salim Chikhi, MISC Laboratory, Constantine 2 University, Constantine, Algeria

ABSTRACT

Negative Selection Algorithm (NSA) is one of the widely used techniques for Intrusion Detection Systems (IDS) designing. In this paper, the proposed is an IDS based on a new model of NSA namely HNSA-IDS (Hybrid NSA for Intrusion Detection System Adaptation). The proposed system can detect unknown attacks; moreover can be adapted automatically when new profiles’ changes of the system are detected. To determine the efficiency of the proposed approach, the standard KDD99 dataset was used for performing experiments. The obtained results show that the authors’ mechanism outperforms some literature techniques providing variant important properties as high detection rate, low false positive, adaptability and new attacks detection.

Keywords: Adaptability, Immune Artificial System (AIS), Intrusion Detection System (IDS), KDD99, Negative Selection Algorithm (NSA)

INTRODUCTION

The increasing use of online services for shopping, banking, military transaction and other business, makes information security primordial. Confidentiality, integrity, and availability (CIA), the main properties of data stored in computer systems, ensure that only authenticated and authorized entities are able to reliably access secure information.

However, these principles can be violated when vulnerabilities exists in complex software system. These can be discovered and exploited by malicious users to gain unauthorized access to system. To prevent these security compromises, layers of defense use preventative measures in the network include: pass word, proxies, fire-falls, filters… Hosts are also protected through proactive patching using antivirus, and anti-spy-ware technology, eliminating unnecessary services and implementing used authentication and access control.

Since prevention mechanisms are imperfect, a monitoring for security compromises is required. This is the role of an IDS. An IDS aims to detect malicious activity in real time and raises an alert.

DOI: 10.4018/IJISP.2014100101
We distinguish two types of IDS: misuse based systems and anomaly based systems. Misuse based systems uses pattern matching for the analysis. This approach examines network and system activities for known misuses, usually through some form of pattern-matching algorithm. Therefore, the idea behind misuse detection consists of comparing network traffic against a model describing known intrusion events. This approach has proved to be very effective at detecting known threats but largely ineffective at detecting unknown threats (Jungwon, 2007).

On the other hand, anomaly based systems base their decisions on a profile of normal network or system behavior, often constructed using statistical, machine learning or data mining techniques. Any event that does not conform to this profile is considered anomalous (Carlos, 2012). These systems are able to detect new attacks but currently produce a large number of false positives.

Hybrid systems are also considered with the aim to gain the advantages of each approach and to reduce their weakness.

Since its birth, the intrusion detection problem is mostly viewed as anomaly detection or a classification problem in which a given event is assigned as normal or intrusive. So, a variety of statistical, machine learning and data mining techniques have been used in designing and implementing efficient IDS.

The use of artificial immune system (AIS) in intrusion detection is an appealing concept for two reasons. First, the human immune system provides the human body with a high level of protection from invading pathogens, in a robust, self-organized and distributed manner. Second, current techniques used in computer security are not able to cope with the dynamic and increasingly complex nature of computer systems and their security.

The negative selection algorithm (NSA) is one of the most important algorithms of AIS. Due to its ability to distinguish the difference between self and non-self, fits naturally into the area of intrusion detection. So a lot of methods and techniques based AIS have been proposed for the effective engineering of IDS.

Detecting unknown attacks and adaptability are the main properties that are very desired for designing an efficient IDS. In intrusion detection systems it is very known that the system space (normal/abnormal) often varies over time, e.g. the computer administrator always changes the configuration of system or network. Moreover, new attacks can occur. The IDS should then adjust the built profile of the normal and abnormal in real time.

In traditional IDS based NSA is difficult if not impossible to update the profile of the system at the time of detection when new changes are made in the listening environment. Furthermore, the current models of proposed NSA for IDS, needs only normal samples from the training class, where in the detection stage of NSA there are only two classes for a tested sample: normal or abnormal, and no detail of abnormal is given. So these methods cannot build an appropriate profile of the system and lacks adaptability.

It motivated by in many intrusion detection applications, abnormal data is often available at the training stage. For instance, in computer security, it is possible, to obtain data about known attacks, e.g. Benchmarks, honey-Pots, honey-Nets, known attacks signature…).

In the aim to overcome the above problems a new hybrid NSA algorithm for an adaptive IDS termed HAIDS is proposed here. This work mainly focuses on the problem of updating the system profile when a new normal behavior or new attack is detected. Our NSA has two training stages and needs the normal and abnormal samples in the training stages to generate the normal and abnormal self-detectors. These detectors use in the detecting stage to examine an incoming connection and determine in which class is belonging. In our case, there are four classes: known normal connection, new normal connection, known attack and new attack class.

In order to show the detection performance and possible advantages of the proposed mechanism, we performed the experiments using two types of data: synthetic and a real data. Where
Preserving Privacy in Mining Quantitative Associations Rules
[www.igi-global.com/article/preserving-privacy-mining-quantitative-associations/40357?camid=4v1a](www.igi-global.com/article/preserving-privacy-mining-quantitative-associations/40357?camid=4v1a)

The Nature, Extent, Causes, and Consequences of Cyberbullying
[www.igi-global.com/chapter/the-nature-extent-causes-and-consequences-of-cyberbullying/213646?camid=4v1a](www.igi-global.com/chapter/the-nature-extent-causes-and-consequences-of-cyberbullying/213646?camid=4v1a)