Extended Thymus Action for Reducing False Positives in AIS based Network Intrusion Detection Systems

M. Zubair Shafiq, Mehrin Kiani, Bisma Hashmi and Muddassar Farooq
College of Electrical & Mechanical Engineering
National University of Sciences & Technology
Rawalpindi, Pakistan
zubairshafiq@ieee.org, {kiani013,b.hashmi}@gmail.com, muddassar.farooq@udo.edu

ABSTRACT

One of the major problems faced by anomaly based Network Intrusion Detection (NID) systems is the high number of false positives. False positives refer to the false detection of normal behavior as malicious behavior. Artificial Immune Systems (AISs) also fall under the category of anomaly based-NID systems. AIS presented in this paper is as a victim-end filter, consisting of detectors distributed on the network, which distinguishes normal traffic from malicious traffic. In this work, we focus on TCP-SYN flood based Distributed Denial of Services (DDoS) attacks. Light Weight Intrusion Detection System (LISYS) provides the basic framework for AIS based NID systems. AISs normally utilize the negative selection algorithm in thymus action to tolerize the detectors to normal traffic so they may not detect normal traffic as malicious traffic. We propose and implement 'extended thymus action' model to improve this characteristic of AIS. Results verify that our model significantly reduces false positives which is a major concern in anomaly-based NID systems.

Categories and Subject Descriptors

D.0 [**Software**]: GENERAL

General Terms

Experimentation, Performance, Security

Keywords

Artificial Immune System, Network Intrusion Detection

1. INTRODUCTION

NID systems can be classified into two major categories namely signature-based NID systems and anomaly-based NID systems. Signature-based NID systems extract signature from traffic and match it to the stored signatures from a pre-existing library. Anomaly-based NID systems store information about normal behavior and detect deviation from this normal behavior. This allows anomaly-based NID systems to detect such innovative attacks whose signatures are not stored in the library. But major problem with such systems is high number of false positives (false alarms).

GECCO'07, July 7-11, 2007, London, England, United Kingdom.
ACM 978-1-59593-697-4/07/0007.

2. ARCHITECTURE AND RESULTS

Hofemyr and Forrest proposed a basic architecture (known as LISYS) to cater for TCP-SYN flood based attacks in [1]. We propose an extension to basic thymus action model which is responsible for tuning of detectors so they may not detect normal traffic as malicious traffic. In extended thymus action, a randomly generated set of detectors is evolved for multiple generations in thymus [2]. Negative selection principle is used to tolerize detectors to normal traffic. *Generations*, set to a predefined constant, is decremented after every generation. If *Generations == 0*, and detector still has not developed tolerization for self-data, then the detector undergoes programmed cell death, also known as apoptosis. Otherwise detector fields are mutated randomly and are checked for self-match till *Generations == 0* or self-match occurs. The number of self-matches converge to zero for $Generations \gg 1$.

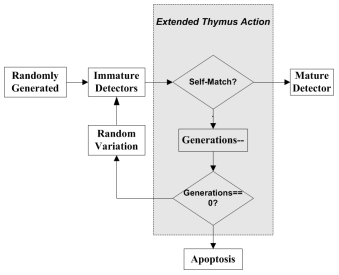

Figure 1: Extended Thymus Action

We compared our approach of extended thymus action to simple thymus action in a well known network simulator OMNeT++. The comparison was done under different attack scenarios with varying degree of malicious activity. The results obtained through extensive experiments clearly demonstrate that the proposed model achieves lower number of false positives in differents attack scenarios as compared to the system not utilizing our model.

3. REFERENCES

[1] Steven A. Hofmeyr and S. Forrest, "Architecture for an Artificial Immune System", Evolutionary Computation Journal, pp. 443-473, 2000.

[2] M. Zubair Shafiq, Mehrin Kiani, Bisma Hashmi, Muddassar Farooq, "Extended Thymus Action for Improving AIS based NID system", Technical Report # 2007/EME-DCE-04, National University of Sciences & Technology, Pakistan.