INTERNATIONAL JOURNAL OF RESEARCH – GRANTHAALAYAH
A knowledge Repository

RACSIT - 17

SURVEY ON SIGNATURE BASED INTRUCTION DETECTION SYSTEM USING MULTITHREADING

Sanjay Roka [*1], Santosh Naik [2]
[*1] 4th Semester CSE, M.Tech. Student, SET, Jain University, Bengaluru, India
[2] Associate Professor, PG Coordinator, SET, Jain University, Bengaluru, India

DOI: https://doi.org/10.5281/zenodo.572296

Abstract

The traditional way of protecting networks with firewalls and encryption software is no longer sufficient and effective. Many intrusion detection techniques have been developed on fixed wired networks but have been turned to be inapplicable in this new environment. We need to search for new architecture and mechanisms to protect computer networks. Signature-based Intrusion Detection System matches network packets against a pre-configured set of intrusion signatures. Current implementations of IDS employ only a single thread of execution and as a consequence benefit very little from multi-processor hardware platforms. A multi-threaded technique would allow more efficient and scalable exploitation of these multi-processor machines.

Keywords: Intrusion Detection; Signature; Multi-Threading.

Cite This Article: Sanjay Roka, and Santosh Naik. (2017). "SURVEY ON SIGNATURE BASED INTRUCTION DETECTION SYSTEM USING MULTITHREADING." *International Journal of Research - Granthaalayah*, 5(4) RACSIT, 58-62. https://doi.org/10.5281/zenodo.572296.

1. Introduction

A signature-based IDS analyzes packets from a computer network and matches them against a set of signatures that trigger on known intruder techniques. In a typical setup, an IDS analyzes all packets flowing through some point in the network. The signature based IDS detects whether the packets match any of its signatures and delivers matching packets to on analysis backend. The performance of the detection process is an important metric in the evaluation of a signature based IDS. An overloaded system will eventually drop incoming packets and fail to scan all traffic. Intrusion detection systems are often implemented in software on general purpose Central Processing Units (CPUs), often on off-the-shelf server hardware. These systems offer high performance at moderate cost, are flexible and allow easy maintenance. However, current signature based IDS are implemented as a single thread of execution and this limits their

performance to the performance of a single CPU, even if this CPU is part of a multi-processor platform.

This survey presented a new approach to improve signature based IDS performance beyond the single CPU performance limit. Small-scale multi-processor computing platforms have been around for a while now and operating system support for them has matured. These platforms are excellent candidates to run a compute-intensive job as a NIDS sensor. To exploit the capabilities of multiple processors, we develop a multi-threaded NIDS sensor. This allows to spread the signature matching workload over multiple CPUs of the same machine and performance to scale beyond single-CPU machines

2. Literature Survey

An IDS is a software application that detects any intrusion in the defined network limits. IDS are differentiated into two types:

1) Host intrusion detection system (HIDS)
2) 2 .Network intrusion detection system (NIDS)

Host intrusion detection system, as the name suggests resides on single host. It examines the activities on an individual host on which it is installed. Login attempts, system log files, resource utilization are analyzed for detection of an intrusion. HIDS may depend on the host's operating system.

Network intrusion detection system collects information from the network traffic stream. This information is compared with signatures to detect sign of an attack. Attack signatures are predefined rules on which will constitute attack. NIDS monitor traffic over a specified network segment and are independent of operating system. Hybrid intrusion detection systems are the one which possess capabilities of both the Host intrusion detection system as well as Network intrusion detection system. In the year 1998, Martin Roesch launched an IDS named "SNORT".

A thread represents as the smallest unit of execution to which a processor allocates time [1]. Multi-threading is a single core or multi-core processor's ability to execute multiple threads at the same time. Although in a single-core CPU one cannot experience the real power of multi-threading but in today's multi-core CPUs or Multi-processor systems, multi-threading plays a crucial role in system performance. A signature-based NIDS analyzes packets from a computer network and matches them against a set of signatures that trigger on known intruder techniques.
In a typical setup, a NIDS analyzes all packets flowing through some point in the network. The NIDS detects whether the packets match any of its signatures and delivers matching packets to on analysis backend. Current NIDS are implemented as a single thread of execution and this limits their performance to the performance of a single CPU, even if this CPU is part of a multi-processor platform. To exploit the capabilities of multiple processors, a multi-threaded NIDS should be used. This allows to spread the signature matching workload over multiple CPUs of the same machine and performance to scale beyond single-CPU machines.

The approach of a multi-threaded NIDS has been explored only partially up till now: some work has been done to separate signature matching on the one hand and output or storage of detected intrusions on the other into different threads or processes running on the same machine [2, 3].

The paper describes an intrusion detection system whose operational ability is derived in correspondence to a human immune system. The IDS presents features such as intrusion evidence gathering, attack signature extraction and automated response against any intrusive activity. Automated response reduces the human effort in ensuring the security of the network [4].

The paper describes functioning of a Network Intrusion Detection System embedded in a smart sensor. The key issues which are addressed and considered for the development of such a NIDS are the number of alerts generated by a traditional IDS and the complexity involved in managing these alerts. As a solution to afore specified issues, a Distributed Intrusion Detection System proves to be a prominent in reducing the involved complexity [5].

3. IDS Types

There are two ways of IDS's. These are

1) Misuse-based IDS and
2) Anomaly-based IDS.

Misuse approach detects the better known attacks that are predefined however fails to identify the unknown attacks. The major advantage of using misuse approach is to produce less false alarms. In anomaly approach, it detects the unknown attacks with high false alarms. Once an anomaly based attack is detected it becomes a signature based or misuse based attack.

Misuse-based or Signature Based IDS

Misuse based IDS is used to detect the known attacks which are predefined. Each of the known attacks are predetermined in the form of signature and are saved, incoming data is matched with their signature to determine the attacks [6]. Misuse-based or Signature Based IDS works when a person sends data to the network. Firstly all data depart to the server and server verify them, if any harmful data is found then server discards the packet else sends it to the network. When the data arrives to server, server uses comparing tool to verify that network packet from the database of signature stored in the server and if server identify the packet that is matched to the database then it discards the network packet else sends the data to the network [6].

Signature based IDS using multithreading contains the following module.

1) Packet Capture Module

This module is responsible for capturing live packets from network. The captured packets are passed to packet preprocessor module. Packet preprocessor module categorizes the captured packets according to protocol like TCP, UDP, HTTP, etc. These packets are then passed to intrusion detector module. The intrusion detector checks for intrusion. If the packet is intruder then the detector creates a log of attack and generates alarm.

2) Intrusion Detection With Multithreaded design Module

Multi-threading is a programming feature that allows multiple threads to exist within the context of a single process. These threads share the resources, but are able to execute independently. The threaded programming model provides a useful abstraction of concurrent execution. The most interesting application of the multithreading is when it is applied to a single process to enable parallel execution. Let us consider, Detection module is a single process that decide whether the captured packet is intruder or not. A single process works well when there is normal traffic in network. However if the network is flooded or traffic is bursty, this will slow down detection process or there is possibility of missing potential attack due to dropping extra packets. To deal with this problem the multithreaded design is considered to be useful. The following algorithm is used to solve the problem using multithreading technique.

```
/*initially
capturedPacketCount=0
threadCount=1
Capacity=N*/
for each captured packet
{
        capturedPacketCount++;
        if (capturedPacketCount==Capacity)
                                        {
                capturedPacketCount=0;
                threadCount++;
                Create new thread ();
        }
```

Algorithm 1.Multithreaing

This algorithm works as follows:

Here, captured Packet Count keeps track of number of captured packets and thread Count will count the number of threads created by Detection process, whereas capacity (N) is a variable that holds the maximum number of packets a single thread can handle. Thread Count is initialized to 1 as first thread will be created and it will wait for first packet. After that it will handle up to N packets. After N packets, new thread will be created to handle further packets i.e. second thread will handle N to 2N packets, third thread will handle 2N to 3N packets and so on.

The technique used in signature based instruction detection is shown in the below figure.

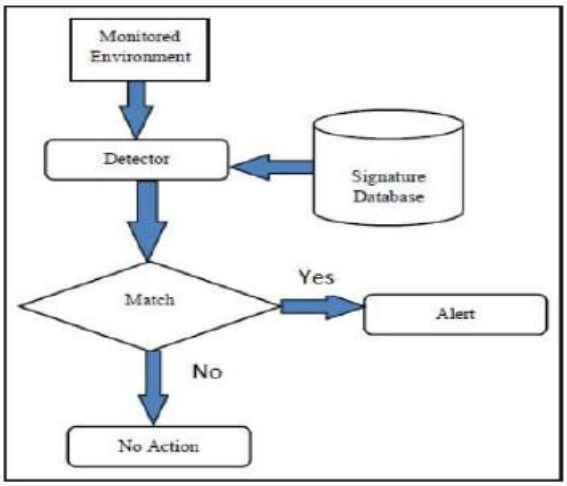

Figure 1: Signature Based Detection Technique

Advantages of Signature based IDS:

1) Alarm is raised when the signature is matched.
2) Signatures are developed based on predefined rules in the tool and depending on the network behavior.
3) Generate low false positive alarm rate.

4. Conclusions

One very effective way to protect networks and personal data from being stolen or alteration, in time, is using IDS system. One of the main challenges almost every IDS systems faces, is the bandwidth growth which results the low performance and attacks can succeed if the system is unable to handle all traffic. Here a multi-threaded solution has proposed to overcome this drawback. This paper further describes about the advantage of using signature based IDS.

References

[1] Lin Gao. "MULTITHREADING", cs9244 report, 2006.
[2] Geschke, D.: Fast logging project for snort. http://www.geschke-online.de/FLoP/ (2004)
[3] Abbas, S.Y.: Introducing multi threaded solution to enhance the efficiency of snort. Master's thesis, Florida State University (2002)
[4] FabricioSergie de Paula, Leandro Nunes de Castro,and Paulo LIcio de Geus, "A Intrusion Detection System Using Ideas from the Immune System ", IEEE 2004.
[5] Francisco Macia -Perez, Francisco J. Mora-Gimeno, Diego Marcos-Jorquera, Juan Antonio Gil-Martinez-Abarca, Hector Ramos-Morillo and Iren Lorenzo-Fonseca, "Network Intrusion Detection System Embedded on a Smart Sensor", Transactions on industrial Electronics IEEE, Vol.58, No.3, March-2011.
[6] Vinod Kumar and Dr. Om Prakash Sangwan, "Signature based intrusion detection system using SNORT", International Journal of computer application & information technology, 2012.

*Corresponding author.
E-mail address: sanjayroka05@gmail.com