A Proposal for Implementation of Signature Based Intrusion Detection System Using Multithreading Technique

Prof.D.P.Gaikwad [1], Pooja Pabshettiwar[2], Priyanka Musale [3], Pooja Paranjape [4], Ashwini S. Pawar[5]

AISSMS'S College Of Engineering,
University Of Pune

Abstract

The rapid proliferation of Internet and mobile computing applications has changed the landscape of network security. The recent denial of service attacks on major Internet sites have shown us, no open computer network is immune from intrusions. 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. In this paper, we are proposing signature based intrusion detection system, using multithreading technique. The multithreading approach will be used to handle network traffic. It takes the advantage of parallel processing on captured packets. We have described the proposal of our multithread based IDS system .We also suggested the algorithm which will help in updating the database which is used for IDS.

Keywords: Intrusion Detection, Multi-Threading, agent.

1. Introduction

Internet is the most important tool for carrying information in people's daily life, in recent years usage of internet has increased tremendously hence network security has become the major concern in computer network. All the computer resources in a network have become vulnerable to potential cyber threats such as network intrusion. To increase network security, use of network intrusion detection systems, firewalls, encryption and other software or hardware solution is immensely increasing.

1.1Intrusion:

An intrusion is an act of intruding in computer network with intent of exploiting system vulnerabilities and having unauthorized access or control over the system.

1.2 Intrusion Detection*:*

Intrusion detection is the process of identifying and responding to malicious activities targeted at computing and networking resources. Intrusion detection systems are of two types [1].

1) Host-based Intrusion Detection System (HIDS)
2) Network-based Intrusion Detection System (NIDS)

1) Host-based Intrusion Detection System (HIDS):

A host-based intrusion detection system (HIDS) is an intrusion detection system that monitors and analyzes the internals of a computing system as well as the network packets on its network interfaces. The target of attackers is systems in corporate network having confidential information. HIDS detects which program accesses what resources and discovers that, for example, a word-processor has suddenly started modifying the system password database. HIDS also detects information present in system and check information is intact i.e. not changed by intruders.

2) Network-Based Intrusion Detection System (NIDS):

In network-based (NIDS), the packets are collected from the network. NIDS monitors network traffic on the network segment for malicious activity and unauthorized access at which it resides. In signature based IDS, signature is a formula that describes an attack. With this method, the system has some kind of knowledge about how attacks look. This means that everything in the system does not explicitly recognize as an attack is considered normal. This is usually solved by using signatures to recognize attacks. This method can be very precise and therefore should have a relatively low false positive rate. False positive is when an alarm is generated although there is no attack. Also known as false alarm. In this paper we are proposing design of signature based intrusion detection system.

2. Literature Survey

We have reviewed various papers of researchers. The contribution of researchers has been discussed below: Ajoy Kumar and Eduardo B. Fernandez [2] have presented a paper on Security Patterns for Intrusion Detection Systems. Intrusion Detection Systems (IDS) play a very important role in the security of today's networks by detecting when an attack occurs. IDS have evolved into an integral part of network security which monitors the network traffic for attacks based , either on existing attack patterns or signatures (Signature-based IDS) or on anomalies or abnormal behavior (Behavior-Based) in the system. They have presented a pattern for abstract IDS that define their general features and patterns for Signature-Based IDS and Behavior-Based IDS.Dr.Sartid Vongpradhip and Vichet Plaimart [3] have proposed survival architecture for distributed intrusion detection system using mobile agent. In this paper they have shown the limitation of present IDS architecture and proposed new architecture that handles intrusion in network and how to survive from it. Mobile agent conceals the major resources in a network topology and network resources are divided into segments. Monitored hosts are installed on each of network segments. The architecture is designed in such a way that when a failure occurs at a single point, then we can recover the vital resources for that point from other systems in the network segments. To guarantee the correctness of message integrity, they made all of communication to pass through only secured channel by using public key cryptography and asymmetric key encryption. Even though proposed architecture can hide important resources of system but the attacker may know the location of proxy agent. So the remedy to overcome this problem is to change the location of proxy agent each time after finishing duty of region agent. Hence it is called mobile agent.Zhang Hu [4] has proposed the new feature pattern matching algorithm which first arranges letters in the pattern string form low appearance probability to high appearance probability, and then match one by one by using existing pattern matching algorithm. This algorithm first matches the rule heads, option heads and then matches the payloads of data packages to find intrusion.

The feature pattern matching reduces the comparison time. In addition to that he has given the detailed description of data acquisition module, protocol processing module, feature pattern matching module, log record module and intrusion response module.Te-Shun Chou [5] has proposed the development of an Intrusion Detection and Prevention system using technique of virtualization. In this paper instead of using real physical equipments in graduate level project of Intrusion Detection system, virtualization technology was employed to build a network with multiple machines running on the single system. In spite of running on the single system, implemented applications and services were executed by virtual machine just as a normal machine would. The advantage of this approach is, it reduces the administrative load and any error can be easily fixed and tackled, this also makes network configuration easy.Mueen Uddin, Kamran Khowaja and Azizah Abdul Rehman [6] have proposed Dynamic Multi-Layer Signature based IDS using Mobile Agents. In case of Signature based Intrusion Detection System each packet needs to be compared with every signature in database to detect an attack, this slows down the process of intrusion detection, especially when network traffic is in rush. Due to this, there is possibility of missing a potential attack. Secondly when a new service or protocol is introduced in a network, network administrator is supposed to update or add signatures into the database but this process is hectic and error prone. Degree of false positiveness is also a major concern in IDS. To overcome aforementioned drawbacks authors have proposed a new model called Dynamic Multi-Layer Signature based IDS using Mobile Agents. They have focused on detecting threats with very high success rate by dynamically and automatically creating and using small and efficient multiple databases. These databases are updated using mobile agents at particular intervals of time.Fang Yu, Zhifeng Chen, Yanlei Diao, T. V. Lakshman and Randy H. Katz [7] have proposed Fast and Memory Efficient Regular Expression Matching for Deep Packet Inspection. In IDS there is need to scan packet contents at high speed. In this paper, authors have shown that memory requirements using traditional methods are very high for many patterns used in packet scanning applications. They have developed a grouping scheme that can compile a set of regular expressions into several engines, which resulted in improvement of regular expression matching speed without much increase in memory usage. Authors have implemented a new DFA-based packet scanner using the above techniques. Their experimental results using real-world traffic and patterns have shown that their implementation achieved a factor of 12 to 42 performance improvement over a commonly used DFA based scanner. Compared to the NFA-based implementation, their DFA-based packet scanner achieved 50 to 700 times speedup.Sarang Dharmapurikar and John W. Lockwood [8] presented hardware-implementable pattern matching algorithm. This algorithm is used for content filtering applications that are scalable in terms of speed, number of patterns and pattern length. For packet content inspection and filtering multipattern matching algorithm is used which detects predefined keywords or signatures in packets. But this algorithm requires lots of memory accesses and is poor in performance. Hence hardware implementable pattern matching algorithm is required. This algorithm is based on memory efficient multi hashing data structure called Bloom filter. They have used on cheap memory blocks in field programmable gate array to construct Bloom filters. These filters reduce a large number of memory accesses and speed up pattern matching. Based on this concept they have presented simple algorithm that scans for several thousands of short patterns i.e. up to 16 bytes with small amount of memory and few megabytes of external memory.

Zhenwei Yu, Jeffrey, J. P. Tsai and Thomas Weigert [9] have proposed An Automatically Tuning Intrusion Detection System. The proposed system will automatically tune the detection model On-the-fly according to the feedback provided by the system operator when false predictions are encountered. This system is evaluated using the KDDCup'99 intrusion detection dataset. Experimental results have shown that the system achieves up to 35% improvement in terms of misclassification cost when compared with a system lacking the tuning feature. If only 10% false predictions are used to tune the model, their system still achieves about 30% improvement. Moreover, when tuning is not delayed too long, the system can achieve about 20% improvement, with only 1.3% of the false predictions used to tune the model. The results of the experiments have shown that a practical system can be built based on ATIDS. Kapil Kumar Gupta, Baikunth Nath, and Ramamohanarao Kotagiri [10] have proposed Layered Approach Using Conditional Random Fields for Intrusion Detection. An intrusion detection system must reliably detect malicious activities in a network and must cope up with the large amount of network traffic; these issues are addressed by authors in this paper. They have demonstrated that high attack detection accuracy can be achieved by using Conditional Random Fields and high efficiency by implementing the Layered Approach. Experimental results on the benchmark KDD '99 intrusion data set shown that their proposed system based on Layered Conditional Random Fields outperforms other well-known methods such as the decision trees and the naive Bayes. The improvement in attack detection accuracy has found to be very high, especially in case of U2R attacks (34.8 percent improvement) and the R2L attacks (34.5 percent improvement). Prof. D.P.Gaikwad and Dr.R.C.Thool [1] have done survey on architecture taxonomy and product of IDS. They mention limitation of various IDS available in market that complete attack prevention is not realistically attainable due to the configuration and administration, system complexity, and abuse by user. They have discussed some aspects of IDS such as role of IDS, categories of IDS, modes of IDS. They proposed the general architecture, network parameter and architectural taxonomy. General architecture consist of three components namely Sensor (agent), Analyzer, User Interface. Sensor collects information and sends it to analyzer. Analyzer determines which intrusion occurs and user interface is used for interaction between system and users. This architecture improves performance of system. They have discussed various features of different IDS's such as Snort, MacAfee and Tripwire. As a future work author are going to develop wireless network IDS system.

3. Proposal Of Our IDS System

We propose the following system which consists of following modules:

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.

Intrusion Detection Module Multithreaded design:

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 we are proposing the multithreaded design. The following algorithm is used to solve the problem using multithreading technique. The our algorithm will work as described below.

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

Algorithm 1.Multithreaing

Here, capturedPacketCount keeps track of number of captured packets and threadCount 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. ThreadCount 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.

Agent and DIDS-

The meaning of a word 'agent' is an agreement to act on one's behalf. In software terms, agent is a program that acts for the user or some other program in a relationship of agency. Thus an agent is attributed to autonomy, authority and reactivity. The concept of an agent provides a convenient and powerful way to describe a complex software entity that is capable of acting with a certain degree of autonomy in order to accomplish tasks on behalf of its host.

Components of Agent

Figure 1 depicts the different modules of agent. Agent consists of 3 modules.

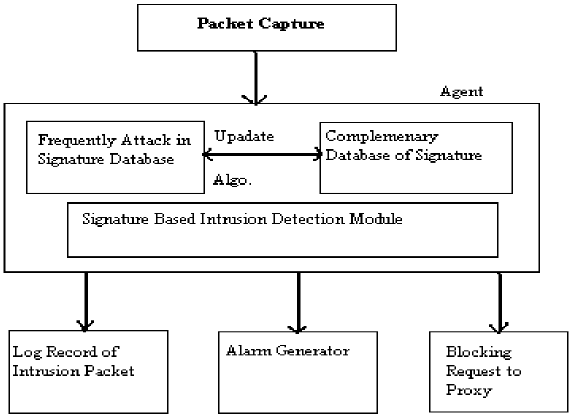
Packet Capture
Agent
Frequently Attack in Signature Database
Upadate
Algo.
Complemenary Database of Signature
Signature Based Intrusion Detection Module
Log Record of Intrusion Packet
Alarm Generator
Blocking Request to Proxy

Figure 1. Modules of Agent

1] Frequent Attack Signature Database: In signature based intrusion detection method, we have a huge database of signatures. In order to check whether the incoming packet is an intruder or not, we have to match the signature of incoming packet against all the signatures in the database. However it is a time consuming process, as the database is large. To overcome this condition, we are using cache mechanism. We are going to maintain a cache of frequently occurring intruder signature database. Complementary database holds all the signatures.

2] Detection Module:

Detection Module is main component of agent. Its main task is to detect intrusion. It works as follows. The detection Module takes packet as input and extracts its signature. This extracted signature is then compared with all the signatures in cached database first, to check for intrusion. If any match occurs then packet is marked as intruder packet, resulting detection in short time. However if no match occurs then the extracted signature is then compared with all the signatures in complementary database. If match occurs then packet is intruder packet otherwise packet is considered to be a normal packet. This module incorporates multithreading logic as aforementioned.

3] Updation Module:

The updation module is responsible to keep frequent attack signature database up to date. The algorithm 2 will used to implement the updation module. This algorithm is used to update this database from complementary database.

```
/* Let
m- max number of entries a frequent attack
database can have
n- number of entries exists in a frequently
attacking database
Initially,
            1] Frequently attacking database is empty.
            2] attackCount field of all entries in
complementary database is initialized to zero
            3] A variable maxOccurance is set to
threshold value.
*/For each record in complementary database
{
  If (count >=maxOccurance)
  {
  Move this record in frequently attacking database
            If (n<=m)
            {
             n++;
            Insert record at n location
    Make its attackCount=0                         }
           Else
          {
            Search an entry in frequently attacking
database with lowest attackCount
            Swap this entry with the selected record
in complimentary database
            Make the attackCount of both records=0;
           }
  }
```

Algorithm 2. For implementation of the Updation Module

We will maintain an attackCount field for each record in frequent attack database as well as complementary database. This variable attackCount will be incremented when intrusion is detected with corresponding record in database. Updation algorithm will work according to attackCount value. This algorithm will run at regular intervals.DIDS: DIDS stands for Distributed Intrusion Detection System. A distributed IDS uses multiple Intrusion Detection modules over a large network, all of which communicate with each other, or with a central server that facilitates advanced network monitoring, incident analysis, and instant attack data. By having these co-operative agents distributed across a network, network analyst and security personnel are able to know what is going on their network. It also allows to efficiently managing its incident analysis resources by centralizing its attack records and by giving the analyst a quick and easy way to spot new threats and patterns. The figure 2 depicts the distributed IDS.

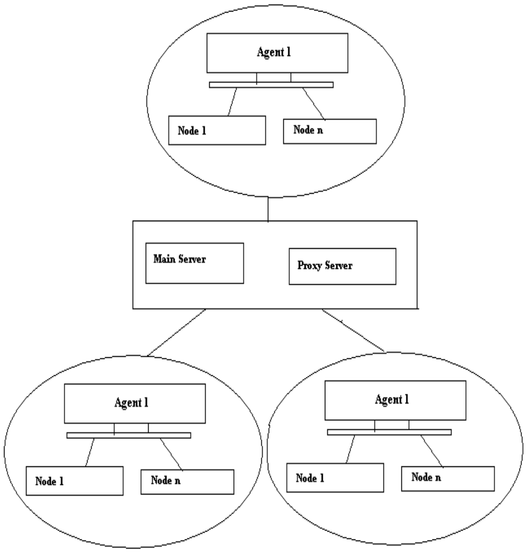

Figure 2. Distributed IDS

The Central Server

The central analysis server is the heart and soul of the operation. This server holds log of all the intrusion data. This allows the interactive querying of attack data for analysis and gives the current attack status of network. It also allows analysts to perform pre-programmed queries, such as identifies attack patterns and performs rudimentary incident analysis.

The Co-operative Agent

The co-operative agent network is one of the most important components. Every LAN in a network has Agent node. All the other nodes in LAN are connected to this agent node. And all the agent nodes are connected to central server. The agent acts in between host node and central server. Each host is having IDS program. Whenever an intrusion is detected, the host reports it to agent and agent forwards this attack information to the central server and proxy server.

The Proxy Server

The proxy server is used in DIDS system with special purpose of blocking Example- if a node has detected that packets coming from source IP address 172.34.34.3 are all intruder packets then it will give notification to agent and agent will request the proxy server to block all the packets with source IP address 172.34.34.3. This will save the time of node for intrusion detection. And deals efficiently with attacks like flooding.

4. Conclusion

The diligent management of network security is essential to the operation of networks, regardless of whether they have segments or not. It is important to note that absolute security is an abstract concept – it does not exist anywhere. All networks are vulnerable to insider or outsider attacks, and eavesdropping. No one wants to risk having the data exposed to the casual observer or open malicious mischief. Regardless of whether the network is wired or wirelesses, steps can and should always be taken to preserve network security and integrity. We have said that any secure network will have vulnerabilities that an adversary could exploit. This is especially true for computer networks. Intrusion Detection can compliment intrusion prevention techniques (such as encryption, authentication, secure MAC, secure routing, etc.) to improve the network security. However new techniques must be developed to make intrusion detection work better for the computer networks. We have shown that a multithreaded technique for better intrusion detection should be distributed and cooperative by applying co-operative agents to the network. Currently, the research is taking place in developing new architecture for NIDS for better security.

5. References

[1] Prof. D.P.Gaikwad and Dr.R.C.Thool, Architecture Taxonomy and Product of IDS.

[2] Ajoy Kumar and Eduardo B. Fernandez, Security Patterns for Intrusion Detection Systems, 1st LACCEI International Symposium on Software Architecture and Patterns (LACCEI-ISAP-MiniPLoP'2012), July 23-27, 2012, Panama City, Panama.

[3] Dr.Sartid Vongpradhip and Vichet Plaimart, Survival Architecture for Distributed Intrusion Detection System (dIDS) using Mobile Agent, Network Computing and Applications, 2007. NCA 2007.

[4] Zhang Hu, Design of Intrusion Detection System Based on a New Pattern Matching Algorithm, 2009 International Conference on Computer Engineering and Technology, 978-0-7695-3521-0/09 DOI 10.1109/ICCET.2009.244.

[5] Te-Shun Chou, Development of an Intrusion Detection and Prevention Course Project Using Virtualization Technology, International Journal of Education and Development using Information and Communication Technology (IJEDICT), 2011, Vol. 7, Issue 2, pp. 46-55.

[6] Mueen Uddin, Kamran Khowaja and Azizah Abdul Rehman, Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents, International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010.

[7] Fang Yu, Zhifeng Chen, Yanlei Diao, T. V. Lakshman and Randy H. Katz, Fast and Memory-Efficient Regular Expression Matching for Deep Packet Inspection.

[8] Sarang Dharmapurikar and John W. Lockwood, Fast and Scalable Pattern Matching for Network Intrusion Detection Systems, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 10, OCTOBER 2006.

[9] Zhenwei Yu, Jeffrey, J. P. Tsai and Thomas Weigert, An Automatically Tuning Intrusion Detection System, IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART B: CYBERNETICS, VOL. 37, NO. 2, APRIL 2007.

[10] Kapil Kumar Gupta, Baikunth Nath, and Ramamohanarao Kotagiri, Layered Approach Using Conditional Random Fields for Intrusion Detection, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 7, NO. 1, JANUARY-MARCH 2010.

[11] M. Salour and Xiao Su, "Dynamic Two-Layer Signature-Based IDS with Unequal Databases", presented at proceeding of the International Conference on Information Technology (ITNG'07), 2007.

[12] Herv´ Debare, An Introduction to Intrusion-Detection Systems.

[13] P. S. Wheeler, "Techniques for Improving the Performance of Signature-Based Network Intrusion Detection Systems," in Computer Science, Davis, CA: University of California, Davis, 2006.

[14] Karen Scarfone, Peter Mell, Guide to Intrusion Detection and Prevention Systems (IDPS), Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930.

[15] Asmaa Shaker Ashoor , Prof. Sharad Gore, Importance of Intrusion Detection System (IDS), International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2011 ISSN 2229-5518.