International Research Journal of Computer Science (IRJCS)
Issue 05, Volume 4 (May 2017) SPECIAL ISSUE
ISSN: 2393-9842
www.irjcs.com

Design and Implementation of Dual Network Security Based Using Signature on Packets

Ashwini M[#1],SukruthaS[#2], Suma Reddy[#3], Syed Zaid Ahmed[#4], Vinay Christopher[#5,]

[#1] Assistant Professor,[1], [#2-5] UG Students.
Computer Science and Engineering,
Vemana Institute of Technology, Bangalore – 560 034

Abstract ***—Intrusion detection system(IDS) work at many levels in the network fabric and are taking the concept of security to a whole new domain by assimilating astuteness as a tool to protect networks against unrestricted intrusions and attacks which are harmful. A well-versed architecture with enhancement of security to a higher level is proposed and presented which gives a higher level of security for an intrusion detection system. The main aim of intrusion detection system is to identify the malevolent activities and to prevent them. The objective of this study is to work with apposite algorithms for intrusion detection and hybrid them to find adequate results and investigate on new hybrid techniques of intrusion detecting system with high accuracy.***

Keywords ***—Intrusion Detection System, Expert System, Signature Matching, Data Mining, Machine Learning.***

I. INTRODUCTION

Intruders which are harmful will come under malicious activities which can either include the intruders from exterior like hackers or intruders within the network. In intrusion detection system, the events are analyzed and monitored in a system or networkwhich are defilements or threats to computer sanctuary policies, suitable strategies, or standard security practices. That system which wits the intrusion in the system is known as IDS (Intrusion detection System). There are several other defence systems such as access control and authentication as a second defence line to protect information systems along with which the intrusion detection system. There are many reasons that make intrusion detection the important parts in the whole defence system. First, many of the outdated systems and applications have been built and developed without taking security seriously into account. Second, computer systems and applications may have faults or bugs in their design that could be used by intruders to attack the systems or applications. Intrusion detection system (IDS) is an amalgamation of software and hardware that challenges to perform intrusion detection protection to normal users and system resources from information security terrorizations. Computer security analysts use intrusion detection Systems to assist them in sustaining computer system security. There were plenteous attacks on software systems result in a process execution or human coding mistakes conflicting from its normal behaviour, all these protruding examples include a malware related code inoculation attacks on internet server's processes and with resulting from buffer surfeit and format string susceptibilities. These are also called anomaly detection techniques because in compare to signature based detection which strays from the normal behaviour are taken as hints of irregularities Support vector machines (SVM) are a conformist of related managed learning methods that analyse data and diagnose patterns, used for classification and regression analysis. SVM delivers a limited solution, since the optimality problem is convex. This is an assistance related to neural networks, which have multiple solutions linked with local minima and for this reason may not be vigorous over different samples. SVM are a set of related directed learning methods that analyse data and recognize patterns, used for arrangement and relapse analysis.

II. EXISTING SYSTEM:

DETECT MALICIOUS ACTIVITIES/ATTACKS

Computer networks are exposed to accumulative number of security threats. With new types of bouts appearing repeatedly. Existing host-based Intrusion Detection Systems use the operating system record or the application record to detect misappropriation or anomaly activities. The hacker or an attacker who attacks the system will take advantage of the flaws of the system. The hacker can either be an official user existing within the system or an intruder from outside.These flaws are specific to a given version and release of the hardware and software on the computer.

RAISE ALARMS

An intrusion detection system inspects all incoming and outbound network commotion and detects suspicious patterns that may designate to a network or a system attack**.** Whenever there is flow of packets from the server to the client it there may be incidence of malicious activities which includes hacking or unauthorised access which may corrupt the network. IDS detect the malicious activities and alerts the admin by raising alarms or trigger defence mechanism if available. The records of all the traffic will be stored for the further orientations as log events. Signatures are allotted to packets which are to be transferred.

LOG EVENTS

Intrusion detection is a process where several events are monitored which takes place in a computer system or network and these events are scrutinized for signs of possible events, these events can either be normal ongoing events orthreats of violation of computer security strategies, acceptable use policies, or standard security practices.Signature-based IDS refers to the detection of attacks by looking for specific outlines, such as byte sequences in network traffic, or known malevolent instruction arrangements used by malware. Signature based detection machineries have little empathetic of many network or application protocols and cannot track and understand the state of complex infrastructures.

DISADVANTAGES:

- *If any malevolent attack occurs, then the packets are blocked from reaching the client.*
- *It is outdated because only RSA algorithm is used.*

III. PROPOSED SYSTEM:

The main aim is to study the behaviour of network and analyse and prevent a malicious node within the network. Application Implants techniques such as encryption as well as signature based security so that whenever there is a communication between server and client by the steps according, approach of authentication is introduced at the client side, when a malicious node gets authentic using SVM helps to map the IP address classify as intruder will not get the comprehensive data which the server is communicating with the client. We are introducing such security to every client present in network, to secure the packets. This can mainly be used in bank applications, many companies for communicating with each other, online transactions etc., where the data plays a very important role btw the server and the client. We are also introducing signature based detection which keeps it verifies the signature.

IV. SYSTEM ARCHITECTURE

A system architecture is a theoretical model that describes the edifice, behaviour, and more views of a system. An architecture portrayal is a formal portrayal and depiction of a system, organized in a way that supports cognitive about the structures and behaviour of the system.

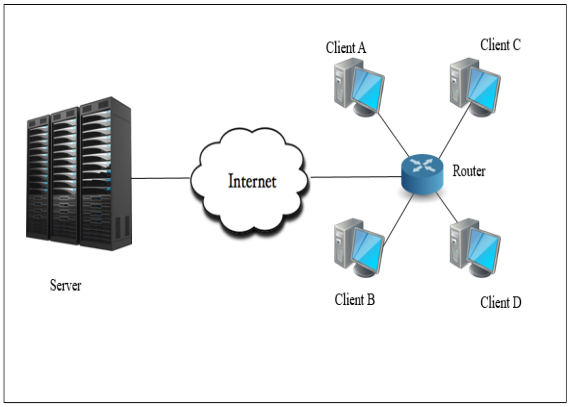

Fig 1: System Architecture of a Network

The above fig describes the system architecture of a network with many clients a server and a router. The flow of packets from client to server is through a network. The server receives the client request and gives the services if available. There are many numbers of clients which creates a basic network. Router performs the circulation pointing functions on the internet. They forward the requested packets to the clients which are sent by the server.

We make use of machine learning and data mining methods like

- *Bayesian Networks- It is a graphical model of a set of arbitrary variables, and the conditional cravings of those variables on each other.*

- *Neural Networks-Used in cases where relationship between inputs and outputs is expected, but the exact relationship between the inputs and outputs is unidentified.*
- *Fuzzy logic-In fuzzy logic, other categories rather than true or false can be used for a set. The truth value of a fuzzy set lies somewhere between 0 and 1.*
- *As RSA algorithm was broken we use the DSA algorithm to obtain more efficient result. Nowadays cyber-attacks are common in the public banking sector, health organizations, defence, and service sector, so organizations are need to give training and strategies, policy adjustments, stepping up awareness programs. So, we prepare effective solutions required to avoid the cyber criminals, viruses, malware. This can mainly be used in bank applications, many companies for communicating with each other, online transactions etc., where the data plays a very important role btw the server and the client. We are also introducing signature based detection which keeps it verifies the signature.*

PROPOSED ADVANTAGES

- *Prevents accessing of files by unlicensed users*
- *Data is received successfully at the destination*
- *Support Vector Machine enhances security in the Network*
- *RSA is used for encryption*
- *DSA is used for Signature based pattern Matching*

V. RESULT & ANALYSIS:

SUPPORT VECTOR MACHINE (SVM)

- Accuracy

1) Results for whole features
The highest AC for the whole features when SVM was used was 94.8000.
2) Incremental results

Figure 2 shows the incremental results when SVM was used as the primary algorithm. The maximum accuracy was around 94 percent while the minimum was around 48 percent. Moreover, when SVM was used, features 1 to 36 had the highest accuracy to detect intrusion while the minimum was when the features of 1 and 2 were used for this algorithm

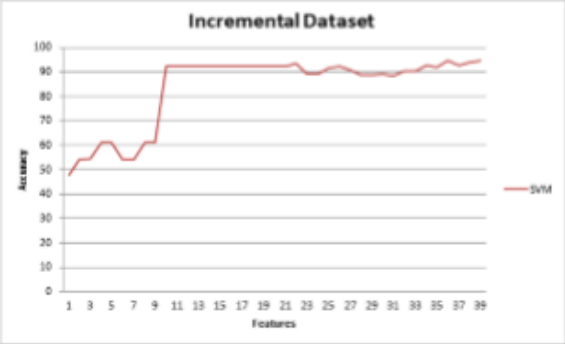

Fig 2: Incremental Results for SVM

- False/True Alarms

TABLE 1. FALSE/TRUE ALARMS FOR SVM

ALARM	True Positive	False Positive	True Negative	False Negative
RATE	98.7500	2.1429	97.8571	1.2500

Table I illustrates the false/true alarms of the SVM. The TP was 98.7500. This meant that the rate of proper attacks was much more than 98 percent. Moreover, the proportion of negative aspects cases which were improperly considered positive namely FP was around 2.1429. In addition, the TN was 97.8571 indicating the amount of ordinary occasions which were effectively called normal. The final results showed the number of attacks which were incorrectly predicted as normal with a rate of 1.2500.

- MSE

The final results of this research using SVM was the MSE with a rate of 0.05220, which showed the amount of error in which the implied value differed from the estimated quantity.

VI.CONCLUSION

This paper defined scenarios which evaluated different algorithms and compared the intrusion detection of these algorithms. Machine learning techniques have received noteworthy consideration among the intrusion detection researchers to discourse the weaknesses of knowledge base detection techniques. Anomaly detection comprises supervised techniques and unsupervised techniques. Many algorithms were used to achieve good results for these techniques. This paper propositions summary of machine learning techniques for anomaly detection. Among the supervised methods, the best performance is achieved by the non-linear methods, such as SVM, multi-layer perception and the rule-based methods. SVM achieved better performance over the other techniques although they differ in their capabilities of detecting all attacks classes efficiently.

ACKNOWLEDGMENT

We would like to express my special thanks of gratefulness to my guide Ms. Ashwini.M as well as our principal Dr. Vijayasimha Reddy who gave us this golden opportunity to do this wonderful project on the topic “DESIGN AND IMPLEMENTATION OF DUAL NETWORK SECURITY BASED USING SIGNATURE ON PACKETS” which also helped us in a allot of research and gain knowledge, secondly we would like to our parents and friends who helped us in finalizing the project.

REFERENCES

[1]. Carter, E., Hogue. J. (2006). Intrusion Prevention Fundamentals (Vol. 1st). USA: Pearson Education, Cisco Press.
[2]. Bail, Y., Kobayashil, H. (2003). Detection Systems: Technology and Development. Paper presented at the 17th International Conference on Advanced Information Networking and Applications (AINA'03), Xi'an, China.
[3]. Sonawane, S., Pardeshi, S., and Prasad, G. (2012). A survey on intrusion detection techniques. World Journal of Science and Technology, 2(3), 127
[4]. Gascon, H., Orfila, A. and Blasco J. (2011). Analysis of update delays in Signaturebased Network Intrusion DetectionSystems. Computers & Security, 30(8), 613-624.
[5]. Devi, S. and Nagpal, R. (2012). Intrusion Detection System Using Genetic Algorithm-A Review. International Journal of Computing & Business Research.
[6]. Burns, D., Adesina, O. and Barker, K. (2011). CCNP Security IPS 642627 (Vol. 1) USA: Cisco Press.
[7]. Nadeem, B. M., Pradeep, K. P. and Kanthi, K. K. (2011). Intrusion Detection in Wireless Networks Using Selected Features. Journal of Computer Science and Information Technologies.
[8]. Owais, S., Snasel, V. and Abraham, A. (2008). Survey: Using Genetic Algorithm Approach in Intrusion Detection Systems Techniques. IEEE.
[9]. Wang, J., Sheng, S., and Chen J. (2009). Polymorphic Worm Detection Using Signatures Based on Neighborhood Relation. IEEE Xplore.
[10]. Yao Y., Y. W., Gao F. and Yu G,. (2009). Modeling the Chaotic Dynamics of Early Worm Propagation. IEEE Xplore.
[11]. Ciobanu, D. (2012). Using SVM for Classification. AUDCE. CCNP Security. Cisco Press.
[12]. Scarfone, K. and Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS) , Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology Gaithersburg, MD 20899-8930.

