Network Intrusion Detection System

Jyoti Mishra ,Grishma Wadhia ,Parth Vasani ,Kunal Iyengar

Jyoti Mishra, Information Technology , Rajiv Gandhi Institute of Technology , Maharasthra , India
Grishma Wadhia, Information Technology , Rajiv Gandhi Institute of Technology , Maharasthra , India
Parth Vasani, Information Technology , Rajiv Gandhi Institute of Technology , Maharasthra , India
Kunal Iyengar, Information Technology , Rajiv Gandhi Institute of Technology , Maharasthra, India

ABSTRACT

Intrusion detection has become a critical component of network administration due to the vast number of attacks persistently threaten our computers. Traditional intrusion detection systems are limited and do not provide a complete solution for the problem. Here we are concentrating and analyzing overall performance as well as security of the proposed ***IDS****. Moreover the proposed* ***IDS*** *approve the effectiveness of the proposed method, and presented results shows advantages of network based security. The proposed model of* ***IDS****s offers several advantages over alternative systems. First of all it provided higher security, it supported high availability and scalability, and most important thing it produced good results in terms of normal and abnormal behaviors of captured packet. The proposed model includes integration of individual components to produced batter results.*

Packet sniffing or packet capture software is extensively used as tools for protocol analysis and security. In protocol design research, such a tool comes handy in analyzing, debugging and testing of a new protocol implementation. In Security, as is true for any tools, it may be used both as a positive way to detect intrusions or attacks on a system as well as in the malicious way to hack for private and personal data of others. Even though use of upper layer encryption techniques make it difficult to gather data directly, yet these tools are important in learning about existing sessions, collecting encrypted data to launch offline attacks to generate the encryption key and any such attack limited only by ones imagination. Packet sniffing is integrated with our project as a key tool to extract the headers of packets to differentiate them from rest of the malicious content.

1.INTRODUCTION

Internet is forcing organizations into an era of open and trusted communications. This openness at the same time brings its share of vulnerabilities and problems such as financial losses, damage to reputation, maintaining availability of services, protecting the personal and customer data and many more pushing both enterprises and service providers to take steps to guard their valuable data from intruders, hackers and insiders. Intrusion Detection System has become the fundamental need for the successful content networking. IDS provide two primary benefits: Visibility and Control . It is the combination of these two benefits that makes it possible to create and enforce an enterprise security policy to make the private computer network secure. Visibility is the ability to see and understand the nature of the traffic on the network while Control is the ability to affect network traffic including access to the network or parts thereof. Visibility is paramount to decision making and makes it possible to create a security policy based on quantifiable, real world data. Control is key to enforcement and makes it possible to enforce compliance with security policy.

1.1TYPE OF IDS USED

Host based IDS (HIDS):

Examines the activity on individual computer or host on which the IDS is installed. The activities include login attempts, process schedules, system files integrity checking system call tracing etc. Sometimes two kinds of IDS are combined to form a Hybrid IDS.

1.2DETECTION TECHNIQUES

Signature/pattern based Detection:

In this technique, the sensors which are placed in different LAN segments filter and analyse network packets in real time and compares them against a database of known attack signatures. Attack signatures are known methods that intruders have employed in the past to penetrate a network. If the packet contents match an attack signature, the IDS can take appropriate countermeasure steps as enabled by the network security administrator. These countermeasures can take the form of a wide range of responses. They can include notifications through simple network management protocol (SNMP) traps or issuance of alerts to an administrator’s email or phone, shutting down the connection or shutting down the system under threat etc.

2.LITERATURE SURVEY

Literature survey reveals that, the Bayesian Analysis is successfully used in the SPAM filters but in the area of IDS it is still not explored to great extent. So in this work, Bayesian classification technique is used for discriminating the anomalous attacks from that of normal activities. Hotelling’s Multivariate statistical hypothesis technique and statistical mean- variances model are also being used. Several information security techniques are available today to protect information systems against unauthorized use, duplication, alteration, destruction and virus attacks. An Intrusion Detection System (IDS) is a program that analyzes what happens or has happened during an execution and tries to find indications that the computer has been misused. There are abundant literatures on Intrusion detection system, and several IDS approaches have been proposed, since the origins of this technology [1-4,61], and as mentioned in Kabiri and Ghorbani [61] and in Abraham [1, 2,3,4]. Two highly relevant works in this direction are given by Denning [27] and Verwoerd. [102]. Dorothy Denning [27] proposed the concept of intrusion detection as a solution to the problem of providing a sense of security in computer systems. The basic idea is that 31 intrusion behavior involves abnormal usage of the system. Different techniques and approaches have been used in later developments. Some of the techniques used are statistical approaches, predictive pattern generation, expert systems, keystroke monitoring, state transition analysis, pattern matching, and data mining techniques. Since 1970, several people have reviewed the state of the art, including: Anantvalee [7], Kabari [61], Bass [16], Jeyanthi and Michel [50, 51, 52], Yang [105], Adam [5], Lee [68], Mukherjee et al. [80], S. Kumar and Lakhotia [96], and Lee. et al [103]. The best reviews are those that present an unbiased, thorough review of the literature, and/or provide a good taxonomy for describing different intrusion detection methods. Examples of such reviews include those by Axelsson [12], Debar [26], Almgren [6], and Hall, M., Jackson wrote an excellent in-depth survey of commercial products. Brumley et al. reviewed defenses against worms [21].

2.1Literature Review

Phillip Brooke, 2006, This paper presents a new IDS framework for mobile adhoc network (MANET) environments based upon the concept of a friend in a small world phenomenon. The two-tier IDS framework has been designed to overcome longer detection mechanisms and detection suffering from the potential for blackmail attackers and false accusations with the help of friend nodes. It is hypothesized that with the introduction of friend nodes, the impacts of the IDS problems can be minimized. It is noted that the proposed framework would not be able to work on a diverse MANET environments.

2.2Market Review

Global intrusion detection system market is expected to grow rapidly during the forecast period. Factors which are driving the growth of global intrusion detection system market are, increasing security threats to enterprise network, growing adoption among IT companies, increasing spending on IT security solution and services and increasing government pressure on compliance of policy and regulations. On the other hand, lack of understanding and awareness about intrusion detection system is a major restraining factor for the growth of intrusion detection system market. However, growing security market in developing economies is expected to create great opportunity for the growth of intrusion detection system market during the forecast period.

On the basis of region, the intrusion detection system market can be segmented into seven regions which includes, North America, Latin America, Western Europe, Asia-Pacific (excluding Japan), Eastern Europe, Japan and Middle East & Africa region. Further the market is sub-segmented as per the major countries of each region in order to provide better regional analysis of the intrusion detection system market. North America region is expected to dominate the global Intrusion Detection System Market during the period of forecast. It is because of high security awareness and increasing government spending on data safety & security. However, growing security market in developing economies expected to drive the growth of intrusion detection market in the region during the forecast period. Asia Pacific region is expected to witness high growth rate during the period of forecast. Furthermore, increasing investment in infrastructure and development of data center by major IT companies, expected to drive the growth of intrusion detection system market in Middle East & Africa region.

Key players in global intrusion detection system market are Tyco International Ltd., Robert Bosch LLC, Corero Network Security, Inc., Extreme Networks, Inc., Juniper Networks, Inc., NSFOCUS, Inc., McAfee, Inc. Nortek, Inc. and Allegion plc among other. Market players are focusing more on new product development and technological advancement as a part of their business strategy.

3.PROPOSED SYSTEM

Despite the fact that intrusion detection systems are commercially developed and used for more than a decade, there still exist many issues around IDS. Some of the shortcomings of the current IDS which handicap its effectiveness are discussed below.

a) Only the known attacks are detected in signature based techniques which simply means no protection is offered against novel attacks or new variants of existing intrusions. A small variation in the attack pattern can invalidate a signature. By the time the new signatures/patches come up the intrusions might have done the intended damages.

b) How well a signature captures the attacks in its string is again a matter of concern. There are quite a few such poorly written signature codes. So the actual attack pattern may stretch across multiple packets, easily evading the detection system.

c) In order to perform an exhaustive signature based search, the processing and memory needs are very high and in the real time scenario, there is quite likely hood of missing genuine attacks. Also, there is the problem of ever increasing attack signature databases.

d) Also the attackers can frame such malicious packets that are likely to have many attack signatures to keep the detection engine busy and in the course of action some packets with real attack patterns will find their way into the internal network, thus evading the detection system

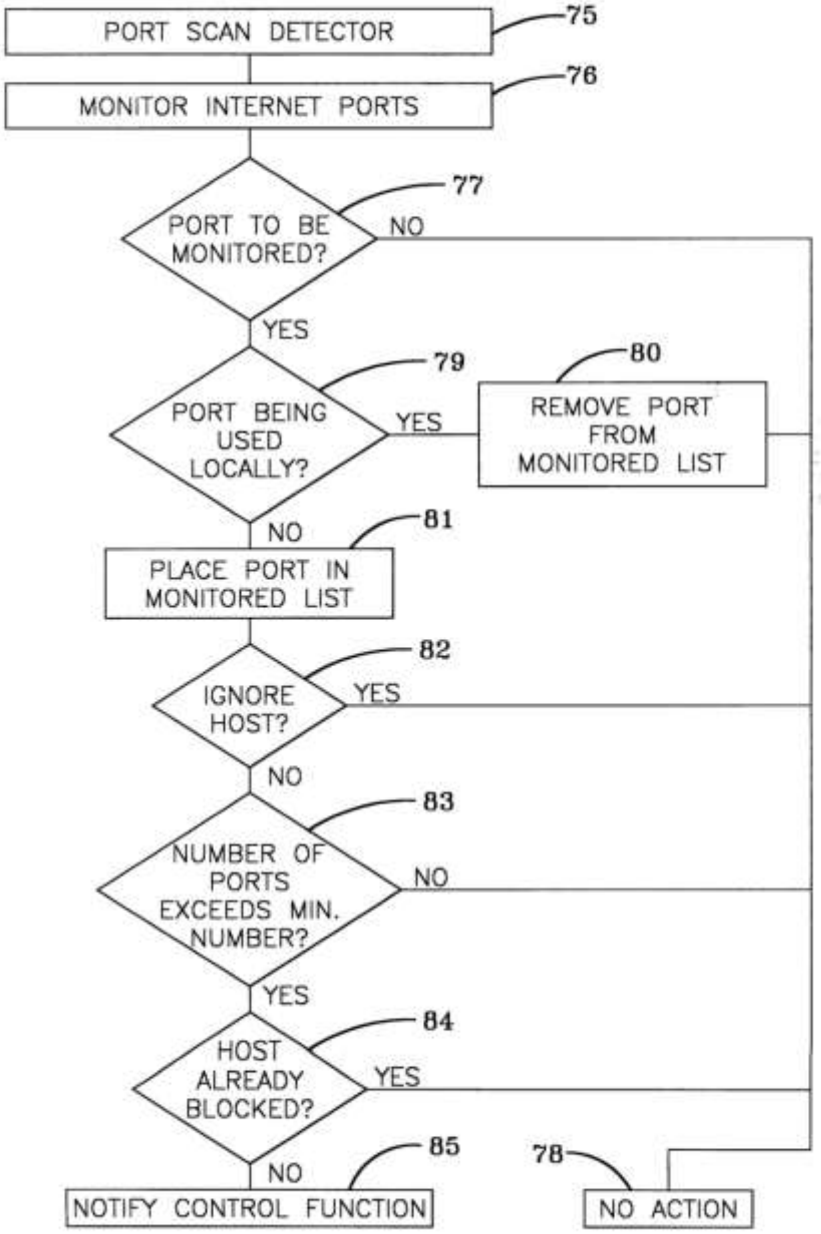
e) There is another class of attacks which targets the detection algorithms as elucidated below. String matching algorithms are the core component of any signature detection mechanism and there is not a single string matching algorithm which can be efficient in any given situation. So the sly intruders can fabricate and send the packets which cause the algorithms to run in the worst case complexities.

f) And what if the attacker sends packets with signatures spread across multiple packets, use techniques like stealth scanning.

g) In anomaly approach, though new kinds of intrusions are detected, this benefit is paralyzed by high number of false alarms. More over improper/ insufficient training to anomaly module results in showing the genuine changes in the network traffic pattern as suspicious activities only

to raise the number of false positives and false negatives.

This intrusion detection system monitors individual systems upon the network. In this case, the sensor of the IDS is located inside of the particular host to monitor system-level behavior. This type of intrusion detection is especially useful for monitoring potentially dangerous user activity within the network. It’s clear that there are two types of host-based intrusion detection software: host wrappers (or personal firewalls) and agent-based software. Here describes the host wrappers as tools that can be configured to look at all network packets, connection attempts, or login attempts to the monitored machine. The agent-based software has the same abilities as the host wrappers, but can also detect changes in system files and changes in user privileges. A report by Network Associates makes a good argument for host-based intrusion detection, stating, and any masking techniques such as insertion, padding, fragmentation, or out-of-sequence delivery, which would evade a network-based IDS can be easily caught by a hostbased IDS." Additionally, host-based IDSs can be quite effective in switched environments, whereas network-based IDS systems are less effective in that environment. A switch tends to isolate communications on the network, making it difficult for network-based IDS to monitor all traffic. However, if the systems on the switched network have host-based IDSs installed, potential attacks may be thwarted.



3.1METHODLOGY

Below are the steps involved in the System Development Life Cycle. Each phase within the overall cycle may be made up of several steps.

Step 1: **Software Concept**

The first step is to identify a need for the new system. This will include determining whether a business problem or opportunity exists, conducting a feasibility study to determine if the proposed solution is cost effective, and developing a project plan.

This process may involve end users who come up with an idea for improving their work. Ideally, the process occurs in tandem with a review of the organization's strategic plan to ensure that IT is being used to help the organization achieve its strategic objectives. Management may need to approve concept ideas before any money is budgeted for its development.

Step 2: **Requirements Analysis**

Requirements analysis is the process of analyzing the information needs of the end users, the organizational environment, and any system presently being used, developing the functional requirements of a system that can meet the needs of the users. Also, the requirements should be recorded in a document, email, user interface storyboard, executable prototype, or some other form. The requirements documentation should be referred to throughout the rest of the system development process to ensure the developing project aligns with user needs and requirements.

Professionals must involve end users in this process to ensure that the new system will function adequately and meets their needs and expectations.

Step 3: **Architectural Design**

After the requirements have been determined, the necessary specifications for the hardware, software, people, and data resources, and the information products that will satisfy the functional requirements of the proposed systemcan be determined. The design will serve as a blueprint for the system and helps detect problems before these errors or problems are built into the final system. Professionals create the system design, but must review their work with the users to ensure the design meets users' needs.

Step 4: **Coding and Debugging**

Coding and debugging is the act of creating the final system. This step is done by software developer.

Step 5: **System Testing**

The system must be tested to evaluate its actual functionality in relation to expected or intended functionality. Some other issues to consider during this stage would be converting old data into the new system and training employees to use the new system. End users will be key in determining whether the developed system meets the intended requirements, and the extent to which the system is actually used.

Step 6: **Maintenance**

Inevitably the system will need maintenance. Software will definitely undergo change once it is delivered to the customer. There are many reasons for the change. Change could happen because of some unexpected input values into the system. In addition, the changes in the system could directly affect the software operations. The software should be developed to accommodate changes that could happen during the post implementation period.

4.CONCLUSION

Network Intrusion Detection System has a major role to play in safeguarding the network resources against various kinds of attacks. With the advent of new vulnerabilities and sophistications in the nature of attacks, new techniques for intrusion detection have evolved. The main objectives of the research being increasing the detection accuracy while keeping the false positive rate low.

As stated earlier, the signature based techniques are good but has the obvious short comings like failure to detect novel attacks, increasing signature database etc. So the viable alternative would be to analyze the behavior of the network as a whole and trying to build the model based on the observations. So Anomaly based detection has been a wide area of interest for researchers since it provides the base line for developing promising techniques. The Anomaly based detection complements the Signature based technique and helps in identifying the novel attacks which lead to the anomalies in the network traffic. The major concerns in this method are identifying the appropriate network features to characterize the network and build a behavioral model and

also the rate of false positives may increase sharply if the IDS is not trained sufficiently in the target network.

5.REFERENCES

[1]. R.Coolen, *"Intrusion Detection: Generics and State of the Art"*, RTO Technical Report 49, http://www.tno.nl/instit/fel/div2/resources/rto-tr-049-ids.pdf

[2]. J. P. Anderson, *"Computer Security Threat Monitoring and Surveillance"*, Technical Report April 1980, http://csrc.nist.gov/publications/history/ande80.pdf

[3]. Martin Roesch : *"Snort Documents"*, http://www.snort.org/docs/

[4]. Net Optics, Inc. *"White Paper: Deploying Network Taps with Intrusion Detection Systems",* http://www.netoptics.com/products/downloads.asp?PageID=150&Section=res

[5]. Jack Koziol, *"Intrusion Detection with Snort"***,** Pearson publications, 2003

[6]. Basic Analysis and Security Engine project, http://base.secureideas.net/

[7]. White papers on *"Basic Analysis and Security Engine"(BASE)*, http://whitepapers.techrepublic.com.com/abstract.aspx?docid=266711