Analysis of recent trends in Intrusion Detection System

[1]Megha Rawat, [2] Deepak Umredkar, [3]Yash Shivhare

Research Scholars
Information Technology Department
Dronacharya Group of Institutions, Greater-Noida, U.P, India

***Abstract*— The study of intrusion detection systems (IDSs) has great importance in the computer science field. In this paper we give a review of recent trends in IDS and challenges related shivhareyashto it. Though there are a number of existing literatures to IDS issues, we have elaborated the most recent trends. The aim of the paper is to help the future researchers to represent a pathway for the exploring the scope of Intrusion Detection techniques and challenges related to this system.**

***Index Terms*— Intrusion Detection, Recent Trends, Challenges, DoS, IDS**

I. INTRODUCTION

In the 21st era the growth of broadcastings networks has taken giant leaps from circuit and packet switched networks towards all-IP based networks. This expansion has created a combined atmosphere. So there security is also an important issue. When taken into account that threats are becoming more and more refined it also means that the security systems have to become more intelligent. A network intrusion detection system (NIDS) [1], [3] monitors circulation on a network (fig.1) considering for suspicious activity, which could be an attack or unsanctioned activity. A large NIDS server can be set up on a strength system, to observe all traffic; or smaller systems can be set up to monitor traffic for a particular server, switch, gateway, or router. In addition to observing the flow of arriving and departing network traffic, a NIDS server can also scan system files looking for illegal activity and to preserve data and file reliability. The NIDS server can also detect changes in the server core machineries.

In addition to traffic monitoring, a NIDS server can also scan server log files and aspect for apprehensive traffic or usage patterns that match a typical network compromise or a remote hacking attempt. The NIDS server can also play an anticipatory role instead of a defensive or reactive function. Possible uses of NIDS include scanning local firewalls or network servers for prospective exploits or for scanning live traffic to see what is actually going on. The important aspect of NIDS server is that it does not replace primary safety such as firewalls, encryption, and other verification methods. One of the main apprehensions is to make sure that in case of an interruption attempt, the system is able to perceive and to report it. Once the recognition is dependable, next step would be to defend the network (response). Hence, the IDS system can be transformed into an Intrusion Detection and Response System (IDRS). Even though researchers are continuously busy in working on both detection and respond sides of the system, a major problem in the IDS is the guarantee [2] for the intrusion detection. This is the reason why in many cases IDSs are used together with a human expert. In this way, IDS is actually helping the network security officer and it is not consistent enough to be trusted on its own. The reason is the incapability of IDS systems to detect the new or altered attack [12] patterns.

II. RECENT TRENDS IN INTRUSION DETECTION TECHNIQUES

The initial step in securing a networked structure is to detect the attack. Even if the system cannot prevent the invader from getting into the system, noticing the intrusion will deliver the security officer with treasured information. Intrusion Detection (ID) can be measured to be the first stroke of defence for any security system. In this section we discuss recent trends in intrusion detection techniques.

Artificial Intelligence and Intrusion Detection

Artificial intelligence is commonly used for the ID purpose. Researchers have projected several techniques in this regard. Some of the researchers are more fascinated in applying rule based approaches to identify the intrusion. Data mining is another approach used by some researchers to resolve the intrusion detection problem using the association rule. Others have proposed application of the concept of fuzzy [11] logic into the intrusion detection problem region. Some researchers even used a multidisciplinary approach; they have combined association rule, fuzzy logic, and genetic algorithm techniques in their effort, where fuzzy logic and Hidden Markov Model (HMM) have been positioned together to detect intrusions. In this approach HMM is used for the dimensionality lessening. Some researchers used the Bayesian [9] methodology to solve the intrusion detection problem. The main idea behind this approach is to find the reason of the actions for a given significance, by moving back in period using the

probability calculations. This feature is appropriate for finding the reason for a specific inconsistency in the network behaviour. By means of Bayesian algorithm [9], system can somehow move back in time and discover the reason for the events. This algorithm is occasionally used for the clustering purposes as well. In Artificial Neural Network (ANN) [13] based approach an unsupervised classification methods is used to overwhelm the curse of dimensionality for a huge value input features. Subsequently the system is complex and input features are frequent, clustering the events can be a very time consuming task. The Principle Component Analysis (PCA) [13] or Singular Value Decomposition (SVD) [13] methods can be an alternative solution. Some researchers have proposed new data reduction approaches by implementing the data mining methodology. To solve the high dimensionality problems data compression can be considered to be an alternative approach. Generation of association rules, is an alternative to reduce the size of the input data (Rule based approach). Size and dimensionality of the feature space are two major problems in IDS advancement. At the same time, techniques such as Bayesian and HMM that use statistical or probability calculations can be very time consuming. Besides the dimensionality reduction or the data compression methods, there are two other methods that can contract with the problem of calculation time. These methods are explained in the following subsections.

Embedded Programming and Intrusion Detection

First approach is to pre-process the network evidence using a pre-processor hardware (front-end processor). In this approach some parts of the processing is accomplished prior to the IDS. This pre-process will significantly reduce the processing load on the IDS and accordingly the main CPU. A similar task can be done by programming the Network Interface Card (NIC). This approach is useful in many fields including smaller computational traffic and greater performance for the main processor. Implementing this approach will make it easier to identify variation of attacks such as Denial of Service (DoS) attack.

Agent Based Intrusion Detection

Another i.e. second approach is the agent based computing. In this approach not only the workload will be distributed between the separate processors, but also the IDS will be able to attain a complete acquaintance of the networks working condition.

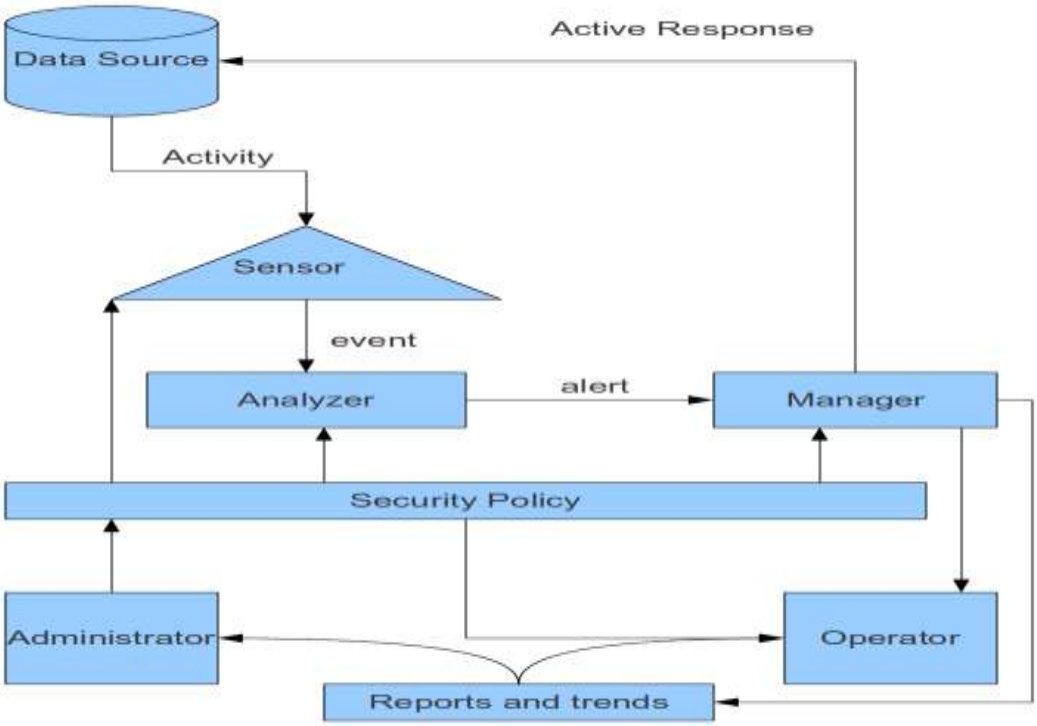

Fig.1. Network Intrusion detection system

Having a complete view of the network will help the IDS to detect the intrusion more accurately and simultaneously it can respond to the threats more effectively. In this approach, servers are interconnected so they can communicate with each other and can alarm each other, in order to respond to an attack. Sometimes it can be adequate to disconnect a subnet when it responds to the attack. In this type of system in order to having a threat, the distributed IDS can instruct severs, routers or network switches to disconnect a host or a subnet. One of the apprehension with this type of system is the additional workload will enforce on the network arrangement by the IDS. The interaction between the different hosts and servers in the network can produce an imperative traffic in the network. The distributed approach can expand the amount of work of the network layers within the hosts or servers and subsequently it may slow them down. There are two approaches to instrument an agent based technology. In the first approach, independent distributed agents are used for both monitoring and communicating. Monitoring the system and communicate with other agents in the network. A Multi-agent grounded system will enjoy a well observation of the world neighbouring it, a multi-agent grounded IDS has four types of agents: Basic agent, Coordination agent, Interface agents, and Global Coordination agent. Each one of these four agents performs a dissimilar task and has its own subsections. These

subdivision agents correspondingly work on the workspaces of the network, and also, the subnet level and unrestricted server level (Mail agent or FTP agent). Thus like this, the complex structure will breakdown into much simpler systems and will become easier to handle. In the second approach, the main goal is to collect information or to perform some tasks which are done by mobile agents they used to travel through the network. The task performed by the mobile agent's IDS are, both the port scanning and the integrity tests on the precarious files of the system. The recommended agent based IDS will raise the alarm if it detects any variation on the precarious files of the system. Other systems can also run by the mobile agents to monitor strength of the target system and to accumulate information.

III. DESIGN TRENDS IN INTRUSION DETECTION

Intrusion Detection System has a classifier kernel. The IDS's kernel is accountable for categorizing the acquired features into two groups namely ordinary and abnormality, where the abnormal pattern is probably be an attack. Nevertheless, there are incidents where a genuine use of the network resources may lead to a positive arrangement of result for the anomaly or signature based intrusion detection. By this incorrect arrangement, IDS will wrongly raise the alarm and will indicate an attack. This is a general difficult situation with the IDS and is called False Positive (FP). One of the constraints to measure the superiority of an IDS is the number of its FP alarms. The smaller is the number of these FP alarms, the enhanced is the IDS. In the following subsections we represents recent design trends in IDS.

Anomaly Based IDS:

In *anomaly based detection [5]* approach, the basic knowledge behind this approach is to learn the standard social pattern of the network. When the network behaves out of its regular actions consequently the attack is suspected (detected). However, network systematic behaviour is not related for different networks. The network behaviour is reliant on the date or the working environments in the corporation where the network is set up and installed. The consistent behavioural prototype for the network can be flexible. Considering these working environments, the level of freedom for the problem is huge. One method to solve this problem is to create the IDS adjustable to the network situation where it is going to be installed. To do so, IDS will start to observe and record the network performance just after its deployment.

Signature Based IDS

Sign based intrusion detection (misuse detection) is one of the universally used and yet precise methods of intrusion detection. When a new attack is hurled, the attack configuration is carefully studied and a sign is defined for it. The sign can be a name (in characters) inside the frame of the attack code, the targeted properties during the attack or the way these properties are targeted (attack pattern). Reviewing the attack's configuration, security specialists can design a system or software that will provide protection against that attack. Later on, using the recommended security method, the IDS is modernized consequently to diagnose the new attack patterns and to react appropriately to them. This approach is very proficient for the identified attacks and generates small number of FP alarms. However, as the major defect of this approach, it is not skilful of detecting new attacks. Once the attack pattern is marginally changed, this approach will not detect the changed forms of the previous attacks. Hence, this approach is only effective in identifying previously known attacks.

Specification Based IDS

An approach is the specification based intrusion detection approach. Some reported works accentuate only on the signature (misuse) based and anomaly based intrusion detection methodologies. However, there are others who talk about all three of the approaches. The specification restriction in this method remains used for dropping the number of FP alarms. In depth knowledge of the system we require implementation of the anomaly based IDS. The specification restrictions are obtained by the human experts manually. Even though specifying critical resources of the system and their employment may advance the security, there are some points that may affect the system utilization which might always be missing in this process. Specification based IDS is not just pertinent to the host systems, they can also be useful for the users as well. An authentic user is expected to perform (act) in a convinced way, or it can be specific that a user should act in this manner. This resolution will recuperate the security but with the expenditure of a less appealing user interface. Restricting the user activities and independence may lead to making the application appearance less eye-catching to some users. It is expected to get improved results by smearing specification based ID methods on the system itself.

Network Based IDS and Host Based IDS [4]

The two categories of the IDSs are- Network based and host based systems. The network based IDS is accountable to defend the whole environment of the network from the intrusion. This task asks for overall understanding of the system status and monitoring both the components of the network and the transactions between them. Agent technology plays a significant role in this policy. For a distributed system network is the infrastructure. Therefore, agents are a usual option for this approach. Agent based technology can accomplish many tasks these are Collecting and processing the information within the network, responding to the requirements and commands of the kernel of the IDS or working as a single system.

IV. CHALLENGES IN IDS

There are many challenges [8] an Intrusion Detection System. In this unit we have given the description of few challenges [6],[12] that the organizations come across while installing an intrusion detection system.

Human intervention

IDS expertise itself is experiencing a lot of augmentations. It is therefore very significant for organizations to evidently define their prospect from the IDS implementation. Till now IDS knowledge has not attained a level where it does not involve human intervention. Of course today's IDS technology indorses few robotics means task for which they automatically perform action like reporting the administrator in case of detection of a malicious activity, escaping the malicious assembly for a configurable period of time, dynamically altering a router's access control list in demand to avoid a malicious connection etc. That's why the security administrator must examine the attack once it is detected and reported, determine how it happened, correct the delinquent and take essential and appropriate action to avoid the occurrence of the same attack yet to come.

Historical analysis

It is quiet important factor to observe the IDS logs frequently to carry on top of the incidence of events. Observing the logs on everyday basis is compulsory to investigate the diverse type of malicious happenings identified by the IDS over a period of time. Today's IDS has not yet attained the level where it can afford ancient analysis of the in sensitive actions perceived over a period of time. This is still a manual commotion. Hence it is spirited for an organization to have a distinct incident control and response plan if an intrusion is identified and recounted by the IDS. Also, the organization should have skilled security workforces to manage this kind of circumstances.

Deployment

The achievement of an IDS implementation depends [10] to a large gradation on how it has been positioned. In the design as well as the implementation phase a lot of plan is required. In most situations, it is prerequisite to apply a combination solution of network based and host based IDS to achieve some advantage from both cases. In reality one technology complements the other. Conversely, this decision can vary from one organization to another. A network system based IDS is an immediate choice for various organizations because of its ability to monitor various systems and it is also the fact that it does not need a software to be laden on a production system different from host based IDS. Some organizations implement a mixture of solution. Organizations mounting host based IDS solution needs to keep in mind that the host based IDS software is memory challenging and a processor. So it is very essential to have adequate existing properties on a structure before inaugurating a host based sensor on it

Sensors

It is essential to maintain sensor to administrator ratio. There is no severe rule as such for computing this ratio. To a large extent it depends upon how many distinct types of traffic is supervised by each sensor and in which circumstantial. Most of the organizations install a ratio of 10:1, while some organizations sustain 20:1 and some others pick 15:1. To avoid false positive it is very important to plan the baseline strategy before starting the IDS implementation. An ailing configured IDS sensor [7] may post lots of false positive ratios to the console and even a ratio of 10:1 or at the same time the better sensors to the console ratio can be omitted.

False positive and negative alarms rate

It is difficult for IDS to be ideal generally because network traffic is very much complex. The inaccurate outcomes in IDS are divided into two forms: false positives and false negatives. False positives occur when the IDS inaccurately identify a problem with compassionate traffic. False negatives occur when unnecessary traffic is ignored by the IDS. Both create problems for safety supervisors or consultants and demands that the malevolent threats must be detected forcefully. A large number of false positives are normally more satisfactory but can burden a security administrator with massive amounts of facts to sieve through. However, false negatives do not provide a chance to the security administrator to check the data because it is unnoticed. Therefore IDS is to be implemented so that it should minimize both false positive and negative alarms.

Signature database

A most known policy for IDS in sleuthing intrusions is to evoke signatures of known attacks. The in-built weak points in depend on signatures that are the patterns must be acknowledged first. New threats are often unrecognizable by eminent and popular IDS. Sign can be masked as well. It has been a challenge for the ongoing event between new attacks and detection systems. Therefore the signature database necessarily be up to date, whenever a dissimilar kind of spasm is detected and repair for the same is available.

Monitor traffic in large networks

Network Intrusion Detection System (NIDS) constituents are speckled throughout a network, but many attacks can altogether avoid NIDS sensors by passing through alternate ways in a network if not placed tactically. Furthermore, many IDS merchandises accessible in the market are proficient to discriminate diverse types of attacks, they may fail to diagnose attacks that use various attack sources. Many IDS cannot smartly associate data from numerous sources. Newer IDS technologies must encourage

integrated systems to enhance an overview of disseminated intrusive action. Therefore IDS must be able to effectively observe traffic in a vast network.

V. CONCLUSION

In this paper, we represent an overview of some of the current and past intrusion detection technologies which are being exploited for the detection of intrusive activities against computer systems or networks. Bearing in mind the surveyed literature, it is clear that in order to be able to secure a network against the original attacks, the anomaly based intrusion detection is the best way out. However, due to its irresponsibility there are still difficulties with admiration to its dependability. These complications will lead to in elevation of false positives in any anomaly-based IDS. The dissimilar recognition encounters that affect the decision strategy of IDS employed in an organization are evidently outlined. Were commend to use the new description of the accompany of fuzzy sets where the fuzzy participation value and fuzzy participation function for the counterpart of a fuzzy set are two distinct concepts because the superficial value is not every time calculated from the ground level. This new explanation of fuzzy sets can be categorized to well-organized rule collections. This would help in decreasing the false alarm rate appeared in intrusion detection system.

REFERENCES

[1]. Richard A. Kemmerer and Giovanni Vigna, Intrusion Detection: A Brief History and Overview in SECURITY & PRIVACY, Computer, Volume:35, Issue: 4 ,2002.

[2]. Man-Ki Yoon ,Sibin Mohan ,Jaesik Choi ,Jung-Euan Kim ,Secure Core: A multicore-based intrusion detection architecture for real-time embedded systems in Real-Time and Embedded Technology and Applications Symposium (RTAS), IEEE , 2013.

[3]. Hung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih Lin, Kuang-Yuan Tung, Intrusion detection system: A comprehensive review in Journal of Network and Computer Applications, 2012.

[4].Herve Deba, Marc Dacier, Andreas Wespi, towards a taxonomy of intrusion-detection systems, Computer Networks 31, 1999 pp. 805–822.

[5]. Animesh Patcha, Jung-Min Park, An overview of anomaly detection techniques: Existing solutions and latest technological trends, Computer Networks, vol. 51, pp.3448–3470, 2007.

[6]. Igino Corona and Giorgio Giacinto and Fabio Roli, Adversarial Attacks against Intrusion Detection Systems: Taxonomy, Solutions and Open Issues, Journal of Network and Computer Applications Volume 36, Issue 1, January 2013, Pages 16–24.

[7]. NA Alrajeh, S Khan, B Shams, Intrusion detection systems in wireless sensor networks: a review in International Journal of Distributed Sensor Networks Volume 2013.

[8]. Teresa F. Lunt, A survey of intrusion detection techniques, *Computers and Security*, 12(4):405–418, 1993. Elsevier Advanced Technology Publications, Volume 12 Issue 4, June 1993 .

[9].Nagaraju Devarakonda,V Valli Kumari , Srinivasulu Pamidi , A Govardhan, Integrated Bayes Network and Hidden Markov Model for Host Based IDS , International Journal of Computer Applications (0975 8887), Vol. 41 , Issue 20, March 2012.

[10]. S.Vijayarani and Ms. Maria Sylviaa.S , Intrusion Detection System-A Study , International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, Issue1, February 2015.

[11]. Mostaque Md. Morshedur Hassan, Current Studies On Intrusion Detection System, Genetic Algorithm and Fuzzy Logic ,International Journal of Distributed and Parallel Systems (IJDPS) Vol.4, No.2, March 2013.

[12]. Amrita Anand, Brajesh Patel , An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, August 2012.

[13]. P. Ganesh Kumar and D .Devaraj, Intrusion detection using artificial neural network with reduced input features, ICTACT journal on soft computing, Issue 01, July 2010.