Comparative Analysis of IDS Approaches and their Techniques

Osheen*
Manpreet Singh**
Raj Kumar Singh***

Abstract

With increase in the reliability of today's generation on the computer systems and internet networks, it is important to maintain a secured network around us so as to retain security of data as well as the systems. During recent years, number ofattacks on networks has dramatically increased and consequently interest in network intrusion detection has increased among the researchers. This research paper will provide an overview of the "Intrusion Detection System" as a whole. This paper will focus on the intrusion detection techniques, its approaches, the securities against the intrusions and the challenges to the techniques used against intrusion.

Keywords: IDS (Intrusion Detection System), NIC (Network Interface Card), Threshold, Anomalous

I. Introduction

The network based applications are becoming an attractive target for vulnerabilities which affects all the actors involved to it, be it the owner of the application and the application in itself too. The most common threat to computer security that we are all aware of are the viruses. There is yet another very common or in a specific way the most publicized threat called intrusion.

The concept of intrusion detection was introduced by Anderson in 1980. According to him "An intrusion or threat is a potential possibility of deliberate unauthorized attempts to

- Access information
- Manipulate information, or
- Render a system unreliable or unusable"

Classification:- Anderson also identifies three classes of intruders:-

- **Masquerader:** These are the ones who are not authorized to use the computer and emerge into the systems access controls, exploiting the account they are likely to be outsiders.
- **Misfeasor:** A misfeasor is one who may not have an authority of access and I he/she has an access authority, he/ she misuses privileges. A misfeasor is generally an insider.
- **Clandestine User:** This one seizes control of the system and uses this control evade access controls or suppress audit collection. This user may be an insider or an outsider both.

II. IDS (Intrusion Detection System)

Before any attack could be prevented, it needs to be detected. The research of detecting the intrusions is called Intrusion Detection. Once the intrusion occurs in a system or a network, the intruder can be determined and the attack can be removed so that the future information leak could be prevented and data could be protected from future damage. A basic intrusion detection system is demonstrated in figure:-

The intrusion detection system primarily focuses on four things. First, identifying probable incidents. Second, monitoring information about them. Third, trying to stop them and fourth, reporting them to security administrators in real time as well as non-real time environment.

III. Intrusion Detection Approaches

The studies on intrusion detection have determined three main approaches of intrusion detection namely:

Osheen*
Student, Institute of Information Technology and Management

Manpreet Singh**
Student, Institute of Information Technology and Management

Raj Kumar Singh***
Department of IT, Institute of Information Technology and Management

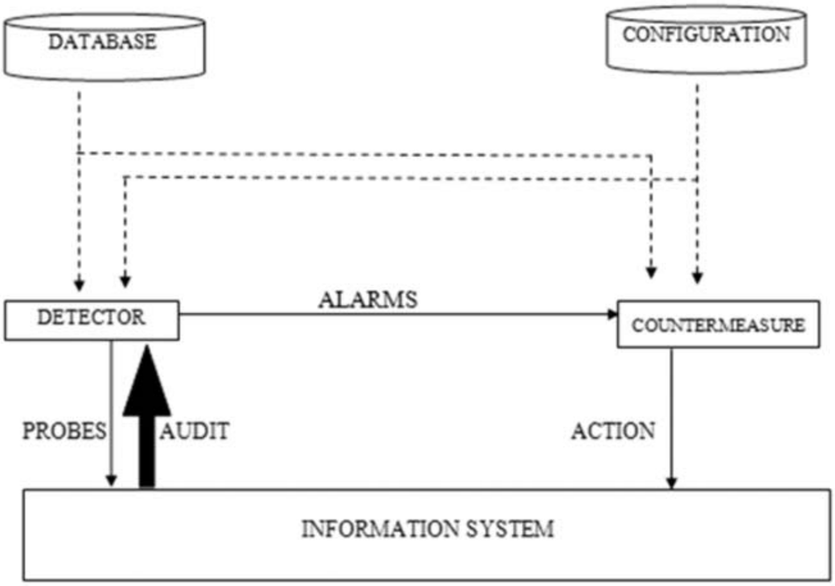

Fig. 1: Simple Intrusion Detection System

[*Source:Mostaque Md. MorshedurHassan "Current Studies on Intrusion Detection System, Genetic Algorithm and Fuzzy Logic"*]

- Statistical anomaly detection
- Rule based detection
- Misuse detection

A. Statistical Anomaly Approach

The statistical anomaly detection approach involves collecting data regarding the behavior of legitimate users over a period of time. After this collection, statistical tests are applied on the observed data to gain a true assurance whether the behavior of the user is a legitimate user behavior or not.The following figure shows a typical statistical anomaly detection approach.

The statistical anomaly detection approach consists of two techniques which are "Threshold Detection and "Profile Based Detection".

Threshold Detection- While performing statistical test, we use flag value. During these tests there occurs possibilities like, the anomaly activities that are not prove to intrusion are flagged as intrusion and The anomalous activities that are prove to intrusion results in false negatives i.e. those activities which are intrusive are not flagged intrusive which are not supposed to occur. For this selection of threshold levels needs to be done which is itself an issue. In this technique, thresholds are defined independent of the user to measure the frequency of occurrence of various events.

Profile Based Detection- In the profile based detection technique; a set of profiles of each user activities is maintained and is used for detecting any change in the behavior of individual accounts. The figure three tells us about the change detected in user profile's activities

B. Rule-based Detection Approach

Rule based detection approach involves a set of rules that are defined to detect the behavior of the intruders.

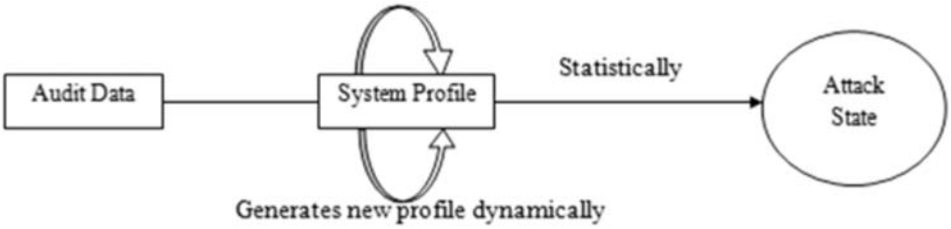

Fig. 2: Typical Statistical Anomaly Detection Approach

[*Source:AurobindoSundaram "An introduction to Intrusion Detection"*]

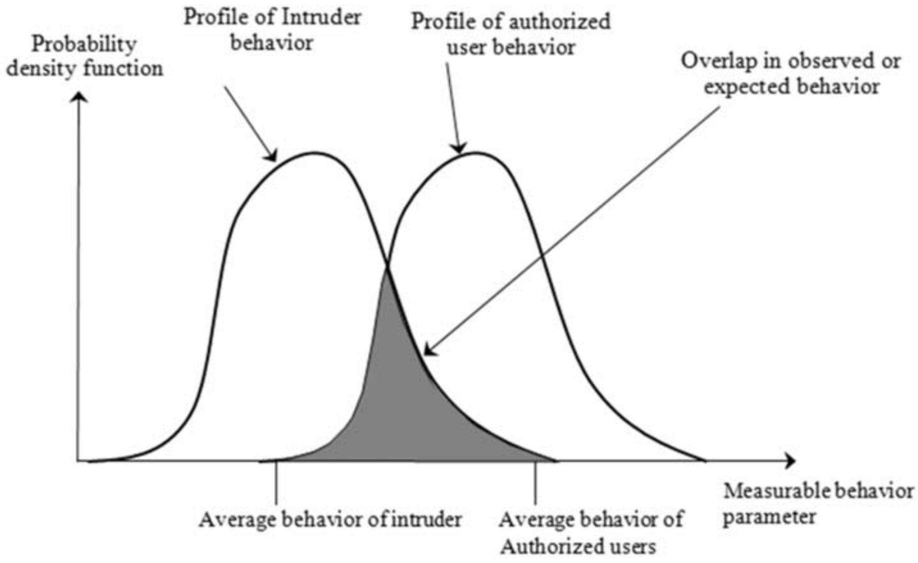

Fig. 3: Profile Activity Behavior of Intruders and Authorized Users

[*Source: William Stallings "Network security Essentials, Applications and standards"*]

The rule based selection approach consists of two techniques which are "Anomaly Detection" and "Penetration Identification".

Anomaly Detection- The rule-based anomaly detection technique is one of among the oldest techniques of intrusion detection and has also been implemented in the recent years. Anderson's report said that the masqueraders and the misfeasors could be detected by monitoring whether the user activities deviates from the normal usage patterns. Thus the anomaly detection providers certain rules which are needed for detection of usage pattern deviation in a user's account.

Penetration Identification- Penetration identification is an expert technique of searching suspicious behavior in a user profile. This technique have become a common supplement in the intrusion detection system. It uses anomaly detection components as well. The penetration identification technique has the capability of detecting the adverse behavior even when the profile confirms to be applying the same usage patterns the way it followed generally.

C. Misuse Detection Approach

Misuses detection technique works on the scheme whose attacks can be represented in the form of patterns and signatures. Even if there are variations of the same attack, it can be detected as the pattern of that kind of attack is already represented. The main difference between the anomaly and misuse detection approach is that the "Anomaly" searches for the complement of adverse behavior whereas the

"Misuse" searches for the known adverse behavior. The figure-4 consists of a typical structure of misuse detection technique approach.

The misuse detection approach consists of three techniques which are "Key Stroke Monitoring", "Model Based Intrusion Detection" and "State Transition Analysis".

Keystroke Monitoring- Keystroke monitoring is a simple technique in which keystroke for every attack pattern is monitored. This technique does not analyze the running program but only keystrokes. This resulted in the flagging the malicious data as intrusive.

Model Based Intrusion Detection- Model Based Intrusion Detection builds up models at higher level of abstraction. They maintain these models of patterns so that the administrator could represent the penetration abstractly. The main goal of this technique is to represent the characteristics behavior of intrusion**.**

State Transition Analysis- In this technique the system monitor is represented as a state transition diagram. As soon as the data is analyzed, the system changes

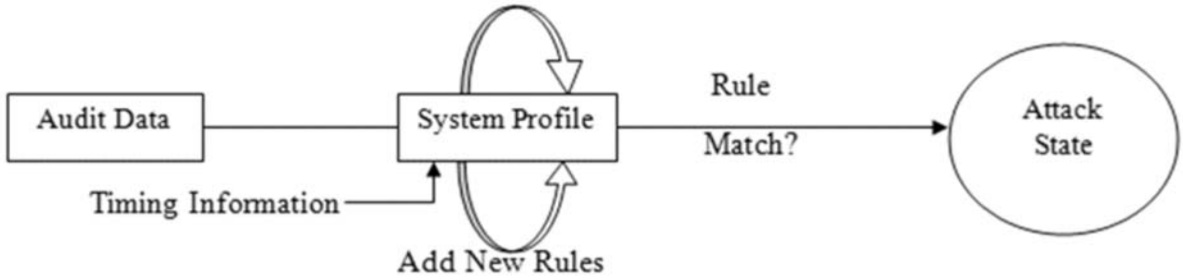

Fig. 4: Typical Misuse Detection Approach
[*Source:AurobindoSundaram "An introduction to Intrusion Detection"*]

from one state to the other. This is generally done when some Boolean condition becomes true. For example- a user when tries to open a file, it checks for its existence which will return true if it exists and then it changes its state from one state to another.

IV. Intrusion Detection Tools

After all the discussed approaches were introduced, now it had to be implemented using some tools. Rather some effective tools which could retain the efficiency of the approaches as well. Certain effective tools for intrusion detection are listed as follows:-

Artificial Intelligence and Intrusion Detection- Artificial Intelligence is a widely used technology for intrusion detection. Some researchers use the statistical approach with artificial intelligence whereas some wishes to use the rule based approach along with it.

Embedded Programming and Intrusion Detection- This kind of technology is one approach in which involves the use of preprocessor hardware or in other words front end processes. In this some parts of the intrusion detection processing is done prior to the IDS to decrease the load of work for the IDS and the CPU as well. This can be done by programming code into the network interface card (NIC) which will be used as the front end processor.

Agent Based Intrusion Detection- In this type of technical approach, the work of detection is divided among the individual processor. This technology not only decrease the work load but also acts as an advantage to the IDS that it can take the whole knowledge of the network working conditions.

Software Engineering and Intrusion Detection- With increase in the complexity of IDS, the complexity of language used to develop the IDS code has also increased, steps have been taken to develop a programming language designed only to develop the IDS code. These languages improve the efficiency of the IDS code as well as the programming speed. The IDS developers can enjoy the benefits of the new language dedicated to the IDS only.

V. Challenges of IDS

Various challenges faced by organizations while installing an intrusion detection system are as follows:

Human Intervention- Till now there is no such IDS installments that do not need human intervention. IDS is itself facing many enhancements due to which the organization needs to explain its prospects for installing IDS.

Deployment- The efficiency of IDS is measured by the way the system is deployed. A lot of planning is required as for designing as well as for implementing the IDS.

False Positive and Negative Alarm Rate- There is a possibility that the IDS may give false alarms. As discussed before, sometimes the IDS may list those activities intrusive which were not and leave those activities which are actually intrusive.

Signature Database- Signature in before is the same as the usage of each attack. The main policy of IDS in detecting is to remember the signature of known attacks. The new threats are often not recognized and hence here is the challenge.

Historical Analysis- Managing and monitoring the IDS log is still a very important task and a necessary task to be done.

VI. Conclusion

All the three approaches namely the statistical anomaly approach, Rule-Based detection approach and the misuse detection system are used depending on the purpose for which the IDS is installed in an organization. Statistical approach being the oldest of all is the most basic form of IDS and is often used in these times for the security while routing whereas the rule-based approach consists of the most expert rules for intrusion detection and provides with the utmost security and the misuse detection approach on the contrary fails to detect unknown intrusions.

VII. Comparative Analysis of IDS Approaches

Approach	Protocols	Application	Advantages	Disadvantages
Statistical Anomaly Detection Approach	Works on the network layer of the TCP/IP protocol, it even help in link state routing protocol.	Counters, gauge-numbers of logical connections assigned to it, resource utilization.	● This approach can adaptively measure user behavior. ● Potentially easy to maintain than rule-based intrusion detection.	● False negative or positive generated depending on the threshold values that can be too high or too low. ● Due to insensitivity of the order of events, relationship between the activities or events is missed. ● It is unknown of what the subset of the possible measure of intrusive activity is.
Rule Based Detection Approach	Works on the DNS network protocol. Works on the rules to create packets, exchange of packets, exchange of packets in a network etc.	Site specific application wisdom and sense (WDS) NADIR.	● Expert rules offers high capability of an odd behavior in the user's account. ● In greater number of rules fired, greater is the suspicious rate. ● Identifies both masqueraders and misfeasors. ● Anomaly detection and penetration identification can be combined together for better security results.	● Needs to be specially crafted to avoid infinite loops. ● There is a possibility of contradictions i.e. under the set of rules for detecting intrusion activity, non-intrusive may fall. ● It can become a complex system as thousands of rules may be needed for detecting first one type of intrusion.
Misuse Detection Approach	Packet analyzer in the network as well as transport layer.	Artificial neutral networks.	● Simplicity of adding known attacks. ● Model based intrusion detection technique in this approach is a very clean approach. ● Noise present in audit data can be filtered which leads to performance enhancements. ● This system can predict attacker's next moves before the attackers thinks of doing	● Inability to identify unknown attacks. ● Does not analyze running programs.

References

1. Amit Kumar, Harish Chandra Maurya& Rahul Misra "A research paper on hybrid detection system"
2. Amrita Anand&Brajesh Patel "An overview on intrusion detection system and types of attacks it can detect considering different protocols"
3. AurobindoSundaram "An introduction to Intrusion Detection"
4. Chintan Bhatt, Asha Koshti, Hemant Agarwal, ZakiyaMalek& Dr. Bhushan Trivedi "Architecture of intrusion detection system with fault tolerance using mobile agent"
5. Dr. Fengmin Gong "Next Generation Inrusion Detection System"
6. Jabez J &Dr. B.Muthukumar "Intrusion Detection System(IDS): Anomaly detection using outlier detection approach"
7. Jeramie Reese "Intrusion Detection System"
8. JP Anderson "Computer Security Threat Monitoring and Surveillance, Technical Report"
9. Karen Scarfone& Peter Mell "Guide to intrusion detection and Prevention System (IDPS)"
10. KoralIlgun, Richard A Kemmerer,Fellow, IEEE and Philip A Porrar "State Transition Analysis: A Rule-Based Intrusion Detection Approach"
11. Mohammad SazzadulHoque, Md. Abdul Mukit& Md. Abu NaserBikas "An implementation of intrusion detection system using genetic algorithm"
12. Mostaque Md. Morshedur Hassan "Current Studies on Intrusion Detection System,Genetic Algorithm and Fuzzy Logic"
13. Parag K Shelke, SnehaSontakke&Dr. A.D Gawande "Intrusion Detection System for Cloud Computing"
14. PeymanKabiri and Ali A Ghorbani "Research on Intrusion Detection and Response: A survey"
15. R.RangaduraiKarthick, Vipul P. Hattiwale&BalaramanRavindran "Adaptive network intrusion detection system using a hybrid approach"
16. Robert S. Sielken& Anita K. Jones "Application Intrusion Detection System: The Next Step"
17. William Stallings "Network security Essentials, Applications and standards"