A Review on Intrusion Detection System based on Artificial Immune System

Pavitra Chauhan
Amity University
Sector- 125, Noida
India

Nikita Singh
Amity University
Sector- 125, Noida
India

Nidhi Chandra
Amity University
Sector- 125, Noida
India

ABSTRACT

Various approaches from different fields have been proposed to improve the security of computer system. One such approach is Intrusion detection system monitors computer system in real-time for activities indicating attempted or actual access by unauthorised users. To build an effective intrusion detection system many techniques are available which gathers and analyze information from different areas within a computer system or network and identify various security threats, including both intrusions anomaly i.e. attacks from outside the organization and misuse i.e. attacks from within the organization. Artificial Immune System (AIS) which is inspired by the robust and flexible nature of Human Immune System (HIS) can be incorporated in current Intrusion Detection Systems (IDS) thereby improving their efficiency and performance. This paper gives a review of various artificial immune system approaches that can be used for the development of an Intrusion Detection System.

General Terms

Intrusion Detection System (IDS).

Keywords

Host based IDS, Network based IDS, Immune System, and Artificial Immune System

1. INTRODUCTION

This paper outlines the necessity of implementing intrusion detection system in the enterprise environment. With the growing use of the computers, a consistent number of the vulnerabilities are also raised constantly. Once these are explored by an attacker, these vulnerabilities put the business and individual users at risk [1].These security issues are rarely given high priority by the software developers, vendors, network managers or consumers. Thus, for protecting the misuse of the systems and for protecting those against attacks Intrusion Detection Systems (IDS) are developed. An intrusion can be defined as any unauthorized attempt to access, manipulate, modify or destroy information[2].An IDS must be capable of identifying "anomalous" behavior and the "misuse" of the computer, thereby also protecting the computer against the network attacks.

For developing efficient IDS, it must be capable of providing various levels of the detection against novel attacks and even variations of known attacks [neural]. For achieving various level of protection, has inspired the use of concepts from Human Immune System. Like human immune system which provides protection to our body from pathogens (i.e. virus, bacteria), the computers must also be provided with similar detection mechanism. Artificial Immune System is inspired from the versatility of the Human Immune System. It is our immune system that let us resist certain infections to which we may be exposed on regular basis.

The rest of the paper is divided into following sections. Section II deals into Intrusion Detection System, Section III having detail about various tools being implemented for intrusion detection, Artificial Immune System is discussed in Section IV, Section V includes the approaches of artificial immune system.

2. INTRUSION DETECTION SYSTEM

Intrusion detection system came into picture around 1980 with the publication of John Anderson's *Computer Security Threat Monitoring and Surveillance*, which was one of the earliest papers in the field. "An Intrusion Detection Model", published in 1987, provided a methodological framework that inspired many researchers and laid the groundwork for commercial products [1].

Intrusion Detection System (IDS) are the popular and useful tools for enhancing the security of the system and because of their value; they have now become a very important part of modern network security technology. Intrusion detection (ID) is a type of security management system for various computers as well as networks. An Intrusion Detection System collects all the information from the Host or the networks which include both anomaly and misuse intrusions. Intrusion detection functions include: 1.) Monitoring and analysing both user and system activities, 2.) Analysing system configurations and vulnerabilities, 3.) Assessing system and file integrity. IDS can be categorized in two ways: one is Host based Intrusion Detection System (HIDS) and another one is Network Intrusion Detection System (NIDS).

2.1 Host based Intrusion Detection system

HIDS is used for monitoring Host based IDS, which is also referred as HIDS, monitors and collects data on the host computer. These data can be either analysed locally or aggregated to another computer for analytical operations. HIDS uses two main approaches "Anomaly Detection" and "Misuse Detection". Anomaly Detection refers to intrusion that can be detected based on anomalous behaviour and use of computer resources. Anomaly detection presumes that misuse or intrusions are highly associated to abnormal action possessed either by a user or a system. Misuse detection techniques attempts to model attacks on a system as a specific pattern, and then systematically scan the system for occurrences of these patterns. Misuse detection uses several approaches but most common are Rule based language, state transition analysis tool kit, pattern matching, TCP/IP protocol analysis and expert systems.

2.2 Network based Intrusion Detection system

Network based IDS, which is also referred as NIDS, monitors and collects data on the network. They scan network streams to detect possible intrusions. This system is potentially very good at detecting unauthorized users even before gaining access to the computer. Network based IDS monitors the whole network traffic and generate the respective output of the analysis. NIDS are these days popular for its efficiency and robustness to detect and prevent attacks over the network. An example of a NIDS is SNORT.

2.3 Passive Intrusion Detection System

When an intrusion is detected, a passive system logs the information and sends an alarm to the administrator or the console does not perform any action on intrusion waits for the administrator’s instruction. The major advantage of such detection system is that they can be build with ease and with a faster pace. Another add on advantage of passive IDS’s is they are not prone to attack themselves. The aim is to detect the potential security breach, log the information and raise an alert.

2.4 Reactive Intrusion Detection System

A reactive IDS (also known as IPS or intrusion protection System) is capable of performing an action in response to the intrusion rather than waiting for anyone to instruct it what to do. Unlike passive IDS, reactive IDSs are designed to give response to activity which harms the system. But on other hand it has some disadvantage like if it has to give response for a suspicious website so it blocks the firewall to pass the information through that site even if it is authoritative.

2.5 Distributed Intrusion Detection System

In this type of IDS there is no central processing IDS acting but instead in a network, at different host there are different IDS employed working isolated to others but can coordinate with each others. This technique decreases detection time by decreasing processing load at one central engine [3]. Another definition of Distributed IDS is that it consists of large number of intrusion detection systems distributed over large network, which communicate with each other or the central server which is responsible for monitoring the network by analysing incidents and generating the related patterns. The scenario of distributed IDS can be visualized by following figure 1 [3].

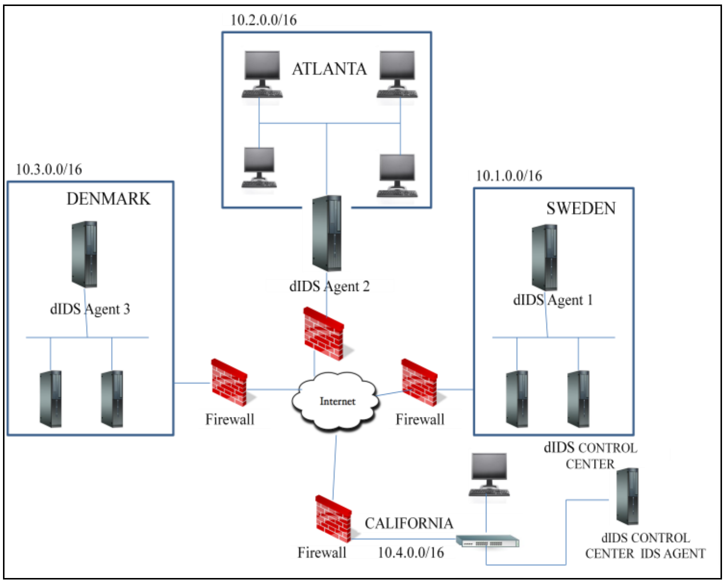

Fig 1: Distributed intrusion detection system

3. TOOLS IMPLEMENTED FOR INTRUSION DETECTION SYSTEM

There are various tools that have been implemented for detecting intrusion in host as well as on network. We have list down around 5 tools that are in the market which specify different role for detecting intrusion.

3.1 OSSEC (HIDS based)

OSSEC is open source host based intrusion detection system. It performs log analysis, integrity checking, Windows registry monitoring, root kit detection, real-time alerting and active response [4]. It runs on most operating systems, including Linux, Open BSD, FreeBSD, Mac OS, Solaris and Windows. It provides with the key benefits such as Compliance requirements, multi-platform, Real-time configurable alerts, integrating with current infrastructure, Centralized management and agent and agent less monitoring. OSSEC Architecture is composed of multiple components. It consist of a central manager who is auditing everything and receiving information from agents, databases, syslog from routers and switches, and from agent less devices. And when some unusual behaviour is detected, active responses are executed and administrator is informed about it. It is advantageous over others since it helps in solving real problems, scalable (because of client/server architecture), easy to customize and is secure by default.

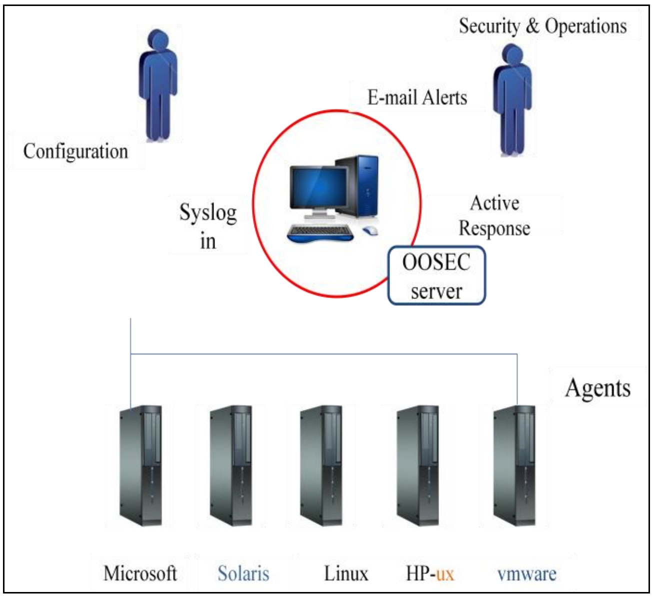

Fig 2: OSSEC Architecture

3.2 Real Secure Server Sensor

It is introduced by IBM Internet Security Systems (ISS) for protecting the business environment from internal and external threats thereby also reducing network costs and down-time. It provides real-time monitoring of the enterprise servers incoming and outgoing activities, and helps in blocking malicious events from damaging the essential assets of the organization [5]. Real Secure Server Sensor integrates with the existing application and enables Policy management and enforcement auditing, Log monitoring, Registry integrity monitoring, OS Auditing and file integrity monitoring. It supports various operating systems such as Microsoft Windows NT 4.0, Microsoft Windows 2000 server, Microsoft Windows server 2003, web and enterprise editions and many more.

3.3 SNORT

Snort is a network analysis tool where it analysis the network and perform detection and prevention of intrusions if any. It was released in 1998 by Source fire Founder and CTO Martin Roesch. It is open source network intrusion detection and prevention system which performs analyses real time traffic in the network. Snort has three primary uses: a straight packet sniffer like tcpdump, a packet logger (useful for network traffic debugging, etc), or a full-blown network intrusion prevention system [6].

3.4 SMART Watch

SMARTWatch is a Host based intrusion detection system which is a pre-emptive hacker Defence tool. It is product of WetStone Technologies which is a security tool builder. It detects the intrusion in resources and can automatically and immediately restore the storage to system resources thus providing uninterrupted system operations. Its latest version comprises of WetStone’s proprietary System Trap technology which has the capability to detect changes in microseconds and immediately restore the damage, and it even automatically notifies personnel in real time, via e-mail or pager [7].

3.5 OSSIM

OSSIM stands for Open source security information management. Its main is to provide a detailed view over each and every aspect of network, hosts, physical access devices and servers. OSSIM is able to work quite efficiently in a various types of environment including Windows, UNIX, network and security devices such as routers, switches, firewalls etc. OSSIM also includes Nagios and OSSEC HIDS [8].

4. ARTIFICIAL IMMUNE SYSTEM

We describe an artificial immune system (AIS) that is distributed, robust, dynamic, diverse and adaptive. It captures many features of the vertebrate immune system and places them in the context of the problem of protecting a network of computers from illegal intrusions. The idea of AIS has been derived from Human Immune system that provides a view to present resistance to disease – causing agents, known as Pathogens (e.g. viruses and bacteria).The main role of immune system is to protect our bodies from infections caused by pathogens. Same way computer security system should protect a machine or set of machines from unauthorized intruders and foreign code, which is similar functionality to the immune system protecting the body (self) from invasion by inimical microbes (no self). Because of this compelling similarity, we have designed an “Artificial Immune system” (AIS) to protect the computer network based on immunological principles, algorithms and architecture.

The biological immune system is highly complicated and appears to be precisely tuned to the problem of detecting and eliminating infections. It is able to categorize all cells (or molecules) within the body as self-cells or non-self cells [9]. It does this with the help of a various mechanisms and barriers that have evolved in order to result in efficient protection. There are two major branches of the immune system which are as follows: The innate immune system is an unchanging mechanism that detects and destroys certain invading organisms, whilst the adaptive immune system responds to previously unknown foreign cells and builds a response to them that can remain in the body over a long period of time. This distinguished information processing biological system has caught the attention of computer science in recent years.

There are certain features of Immune system that give the certain key characteristics that most artificial systems lack: Robustness, Adaptable and Autonomous. The problem of detecting pathogen is often described as that of distinguishing “Self” from “non-self” (which is elements of the body and pathogens). Once pathogens has been detected, the IS must eliminate in some manner.

The innate immune system, also known as non-specific immune system and provides the first line of defence. It comprises of the cells and mechanisms that defend the host from the infection caused by other organisms in a non-specific manner. Cells of the innate system recognize and respond to pathogens in a generic way, but unlike the adaptive immune system, it does not confer long lasting or protective immunity to the host. Innate and adaptive immune system both function to protect against invading organisms. They differ in number of ways [10]:

Table 1. Difference between innate and adaptive immune system

Innate Immune System (Non- specific Immunity)	Adaptive Immune System (Specific Immunity)
Response is antigen-independent	Response is antigen-dependent
There is immediate maximal response	There is a lag time between exposure and maximal response
Not antigen-specific	Antigen-specific
Exposure results in no immunologic memory	Exposure results in immunologic memory

To observe the immune system closely the architecture of human immune system plays an important role in doing the same and its architecture is given below [11]:

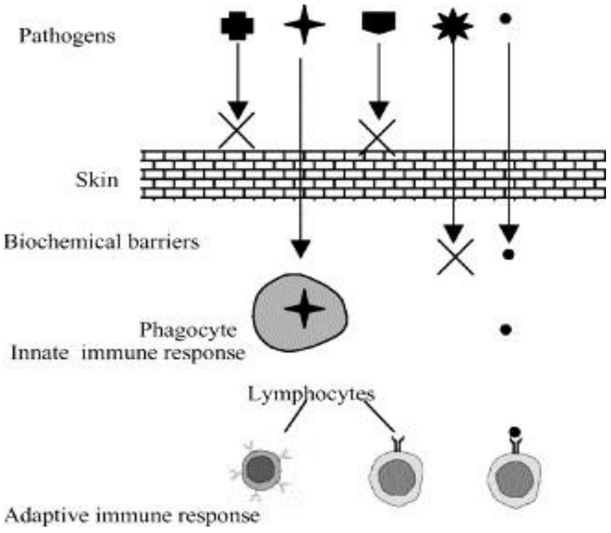

Fig 3: Human Immune System Architecture

The architecture comprises of two parts lower layer handled by Adaptive immune system while a layer just above is managed by innate immune system. The pathogens try to harm the body by penetrating into skin but due to presence of the two layers it is detected and/or prevented. In a similar manner the computer is secured by following the same strategy and thus protecting the system from harmful attacks.

5. INTRUSION DETECTION SYSTEM USING IDEAS FROM ARTIFICIAL IMMUNE SYSTEM

This section explains the various approaches of the artificial immune system that can be used for the implementation of the Intrusion Detection System. Approaches of the Artificial Immune System:

5.1 Neural Network

The Neural Network can be used both for anomaly detection for detecting novel attacks and misuse detection for detecting known attacks and even variation from these attacks. An artificial neural network is composed of simple processing units, or nodes, and connections between them. The connection between any two nodes has some weight, which is used to determine how much one unit will affect the other. A subset of the units of the network acts as input nodes and another subset acts as output node. The activations propagate through the network; a neural network performs the mapping from one set of values to the other set of values. The mapping itself is stored in the weights of the network. This technique was used by Anup.k.Ghosh et al. for building profiles of software behaviour and, thereby distinguishes between normal and malicious software behaviour [12].ANN helps to generalize from incomplete data and to be able to classify data as normal or intrusive [13]. Lin Ying et al. has defined that BP algorithm is an approximate steepest descent algorithm, in which the performance index is mean square error. It is used to train multilayer neural networks. BP is a standard feed-forward network that has been successfully used in other intrusion detection systems as well. There paper implemented host intrusion detection system in which two detection technology one is Log File analysis and other one is BP Neural Network technology. Log analysis is the approach of Misuse Detection and BP Neural Network is the approach of Anomaly Detection. By combining these two technologies HIDS can be implemented effectively and efficiently.

For Misuse Detection, several techniques such as Expert System, TCP/IP protocol Analysis, Pattern Matching can be used. In this paper for Log analysis Pattern Matching was used. For Anomaly Detection, techniques such as Statistical Analysis Methodology, Artificial Neural Network techniques, Data mining and Artificial Immune Technology are used. In this paper for Anomalous behaviour and use of computer resources monitoring, BP (Back Propagation) Neural Network algorithm is used.

5.2 Negative Selection Algorithm

The Negative Selection in an Artificial Immune System is used for network intrusion detection. Jungwon Kim and Peter J. Bentley (2001) observed certain set of requirements for a successful network based IDS and three design goals to satisfy the above stated requirements: being distributed, self organizing and lightweight. An important feature in this paper is that Negative Selection algorithm is inspired by the Negative selection technique of human immune system in which human immune system make use of gene libraries which generate new antibodies from new combinations of gene segments in gene library and avoid antibodies to attack self cells of human body. In this paper they understood the role of important components of artificial immune system for providing appropriate artificial immune responses against network intrusions [14].

5.3 Signature Extraction

A Signature is generated by choosing a pattern that is likely to be found in all the instances of virus. Fabricio Sergio de Paula et al. proposed a framework that is inspired from the human immune system and brings together the desirable features to IDS such as automated intrusion recovery, attack signature extraction and potential to improve behaviour based detection. The prototype is designed to deal with application attacks and extracting signatures. This framework has an advantage that it is extensible to other classes of attacks. Since it is based on human immune system it takes advantage of providing security at various levels. It uses the two basic categories of immune system named as innate immune system and Adaptive immune system which helps in anomaly and misuse detection respectively. Signature extraction is used for the detection of known attacks that is inspired by the concept of adaptive immune system. In this technique encoding of the previous behaviour is done and actions are taken against malicious intrusions. Since this technique prepare signatures of the attack thus, when a similar attack occurs it can be detected easily based on the respective signatures, thereby, avoiding the need to repeat the entire procedure of intrusion detection [15].

6. CONCLUSION

The various IDS tools developed till now were constraint to the detection of known intrusions and most of them suffer from the loop holes. The inability of the IDS inspired us to analyse these tools in such a manner so that we can overcome the loop holes. According to specification of various techniques we observed that by using concepts of artificial immune system we can even detect the unknown attacks. Thus it is believed that if these remarkable features of human immune system are applied to Intrusion detection Systems (IDS), then it would produce highly efficient and versatile Intrusion detection systems which can be referred as Expert Systems.

7. REFERENCES

[1] Anderson, J.P., 1980. Computer Security and Threat Monitoring Surveillance. Technical report at Co. Fort Washington Pennsylvania.

[2] Denning, D. 1987. An Intrusion Detection Model. IEEE Transactions on Software Engineering.

[3] Einwechter, N. An introduction to Distributed Intrusion Detection System. Information available via www.semantic.com

[4] Daniel B. Cid, Rossi, J., Starks, D.P.M., Scott, R.S. OSSEC (Open Source Host-based Intrusion Detection System) http://www.ossec.net

[5] Real Secure Server Sensor tool information available via www at http://www-03.ibm.com/systems/power/software/aix/security/solutions/iss.html.

[6] Roeasch, M. (Chief Technology Officer). Snort (open source network intrusion prevention and detection system (IDS/IPS). http://snort.org/

[7] Hosmer, C. (President and CEO of WetStone). SMART Watch (HIDS Tool). http://www.linuxsecurity.com/content/view/107779/169/ -9

[8] OSSIM tool information available via www at http://sectools.org/tool/ossim/

[9] Vigna, Kruegel, C. 2005. Host-based Intrusion Detection System. In the handbook of Information Security. Volume II John Wiley & sons. -10

[10] Immune System information available via www at http://pathmicro.med.sc.edu/ghaffar/innate.htm

[11] Zheng, H., Zhang, J., Nahavandi, S. 2004. Learning to detect texture objects by artificial immune approaches. Future Generation Computer System. Volume 20.[8]

[12] Anup, K., Schwartzbard, A. A study in Neural Network for Anomaly and misuse Detection. A DARPA funded paper.

[13] Hofmyer, A., Forrest, S. 2000. Immunity by design: An artificial Immune System. Department of Computer science. University of Mexico.

[14] Kim, J., Bently, P.J. 2001. An Evaluation of Negative Selection in an Artificial Immune System for Network Intrusion Detection. In Proceedings of the Genetic and Evolutionary Computation conference.

[15] Sergio de paula, F., Numes de cast ro, L., Licio de gues, P. 2004. An Intrusion Detection system using ideas from Artificial Immune System. In the proceedings of IEEE.

[16] Ying, L., Yan, Z., Yang-Jia, O. 2010. The Design and Implementation of Host-based Intrusion Detection System. Third International Symposium on Intelligent Information Technology and Security Informatics.

[17] Depren, O., Topallar, M., Anarim, E., Ciliz, M.K. 2005. An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks. Expert System with Applications.

[18] Khalkhal, I., Azmi, R., Azimpour-kivi, M., khansari, M. 2011. Host-based Web Anomaly Intrusion Detection System an Artificial Immune System Approach. In the proceedings of IJCSI International Journal of Computer Science Issues. Volume 8.

[19] De castro, L.N., Timmis, J. 2002. Artificial Immune System: A new Computational Intelligence Approach. 1st edition Springer-Verlag.

[20] Hofmeyr S., Forrest, S. 2000. Architecture for an Artificial Immune System. In the proceedings of Evolutionary Computation. Volume 7.

[21] Kim, J., Bentley, P. The Artificial Immune System for Network Intrusion Detection. 7th European Conference on Intelligent Techniques and Soft Computing, Aechan. Germany. 11