World of Computer Science and Information Technology Journal (WCSIT)
ISSN: 2221-0741
Vol. 1, No. 3, 100-104, 2011.

Precluding Emerging Threats from Cyberspace: An Autonomic Administrative Approach

Vivian Ogochukwu Nwaocha
Department of Computer Science
University of Nigeria, Nsukka
Nigeria
ogochukwuvee@gmail.com

Inyiama H.C.
Department of Computer Science
University of Nigeria, Nsukka
Nigeria
drhcinyiama@gmail.com

Abstract— Information Technology and Network Security Managers face several challenges in securing their organization's network due to the increased sophistication of attacks. Besides, the number of attacks and vulnerabilities are rising due to the inability of the existing intrusion detection and prevention system to detect and prevent novel attacks. Hence, intrusion detection systems which were previously adequate to wedge the evolving attacks in cyberspace have become ineffective in impeding these attacks. Consequently, intrusion detection and prevention systems are required to actually prevent attacks before they cause harm. A major consideration of this work is to present an architecture that provides protection through the self-healing and self-protecting properties of the autonomic computing. The proposed system which operates by means of autonomous agents is based on risk assessment. The application of risk analysis and assessment reduces the number of false-positive alarms. Furthermore, the system autonomous features enables it to automatically diagnose, detect and respond to disruptions, actively adapt to changing environments, monitor and tune resources, as well as anticipate and provide protection against imminent threats.

Keywords- Agent; Autonomic Computing; Computer system; Intrusion; Intrusion detection and prevention; Network; Threats.

I. INTRODUCTION

Cyber attack is one of the most rapidly growing threats to the world of cutting edge information technology. As new tools and techniques emerge daily to make information accessible over the Internet, so do their vulnerabilities. Consequently, cyber defence is critical in order to ensure a reliable and secure transmission of information over the internet. Intrusion Detection System (IDS) and Intrusion Prevention and Detection System (IDPS) are the major technologies dominating the field of cyber defence. Although remarkable efforts have been put into intrusion detection as well as intrusion detection and prevention research, the number of network security threats keeps escalating, hence the need to find a solution.

The term intrusion refers to "any set of actions that compromise the integrity, confidentiality or availability of a resource [1]. In the context of Information Security, intrusion detection can thus be defined as the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource. It is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents. When Intrusion detection takes a preventive measure without direct human intervention, then it becomes an Intrusion-prevention system. Intrusion detection can be performed manually or automatically. Manual intrusion detection might take place by examining log files or other evidence for signs of intrusions, including network traffic. Thus, an Intrusion Detection System (IDS) is a device or software application that monitors network and/or information system for malicious activities or policy violations and response to that suspicious activity by warning the system administrator or the process acting on its behalf by one of several ways, which includes displaying an alert, logging the event or even paging the administrator or the acting process [2]. Intrusion Detection Systems can be classified as host-based, or network-based. A host-based IDS monitors system calls or logs, while a network-based IDS monitors the flow of network packets. Modern IDSs are usually a combination of these two approaches. Another significant distinction is between systems that identify patterns of traffic or application data presumed to be malicious known as misuse detection systems, and systems that compare activities against a 'normal' baseline referred to as anomaly detection systems.

Determining what the probable intrusion actually is and taking some form of action to stop it or prevent it from happening again are usually outside the scope of intrusion

detection. Hence, Intrusion prevention is an evolution of intrusion detection. Intrusion prevention is actually the process of performing intrusion detection and stopping known attacks in an instant or attempting to stop detected possible incidents by quarantining or isolation. The Intrusion Prevention System (IPS) is a device or software application that complements IDS and it has all capabilities to stop possible incidents from occurring [2].

Intrusion Prevention Systems (IPS), also known as **Intrusion Detection and Prevention Systems (IDPS)**, are network security appliances that monitor network and/or system activities for malicious activity. They are developed for more active protection to improve upon simple IDS and other traditional security solutions. The main functions of intrusion prevention systems are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity. [3]

Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity.

The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. [4][5] More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address. An intrusion prevention system is the next level of security technology that provides security at all system levels from the operating system kernel to network data flows to data bases [6]. It is primarily designed to protect information systems from unauthorized access, damage and disruption. While an IDS informs of a potential attack, an IPS makes attempts to stop it. Another huge leap over IDS is that IPS has the capability of being able to prevent not only known intrusion signatures but also some unknown attacks due to its KBS of generic attack behaviours and interpreters.

An IPS can also correct Cyclic Redundancy Check (CRC) errors, unfragmented packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options.[4][7]

Intrusion prevention systems can be classified into four different types: [9],[10]

Network-based Intrusion Prevention (NIPS): monitors the entire network for suspicious traffic by analyzing protocol activity.

Wireless Intrusion Prevention Systems (WIPS): monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.

Network Behavior Analysis (NBA): examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations.

Host-based Intrusion Prevention (HIPS): an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

Detection methods

The majority of intrusion prevention systems utilize one of three detection methods: signature-based, statistical anomaly-based and stateful protocol analysis. [5][11]

Signature-based Detection: This method of detection utilizes signatures, which are attack patterns that are preconfigured and predetermined. A signature-based intrusion prevention system monitors the network traffic for matches to these signatures. Once a match is found the intrusion prevention system takes the appropriate action. Signatures can be exploit-based or vulnerability-based. Exploit-based signatures analyze patterns appearing in exploits being protected against, while vulnerability-based signatures analyze vulnerabilities in a program, its execution, and conditions needed to exploit said vulnerability.

Statistical Anomaly-based Detection: This method of detection baselines performance of average network traffic conditions. After a baseline is created, the system intermittently samples network traffic, using statistical analysis to compare the sample to the set baseline. If the activity is outside the baseline parameters, the intrusion prevention system takes the appropriate action.

Stateful Protocol Analysis Detection: This method identifies deviations of protocol states by comparing observed events with "predetermined profiles of generally accepted definitions of benign activity." [5]

II. RESEARCH GOALS

This study seeks to achieve the following goals:

a. Automatically diagnose, detect and respond to disruptions.
b. Actively adapt to changing environments.
c. Automatically monitor and tune resources.
d. Anticipate, detect, identify and protect against threats.

III. RELATED WORK

In recent years, some efforts have been spent to obtain autonomic models that facilitate the protection of computational systems and enhance IT security in exploiting the self-managed feature of agents in the field of intrusion detection and prevention. These provide different levels of protection to assets of a corporation. Albeit with different focus and levels of detail, some works of literature deal with autonomous systems able to manage, evaluate and specify security, either of the information or not, in the most diverse environments. We highlight some of the work that has been done in the area of multi-agent intrusion detection system.

In their work, [12] proposed an autonomic computing architecture for defence in depth information assurance system in a way that the increasing of complexity of the system can be tackled by distributed autonomous security subsystem with the ability of self-configuration, self-optimization, self-healing and self-protection. The system has shown an enormous improvement on the defence in depth information assurance system. The main limitation of the work is lacking the

consideration on risk evaluation and risk assessment. [13] proposed a fuzzy agent-based intrusion detection system based on multi-sensors, where agents use data from multiple sensors with a fuzzy logic to process log files. He considered how Agents represent a new generation of computing systems and is one of the more recent developments in Intrusion Detection Technology. He also explained how agents can reduce the intrusion detection workload by sifting through large amounts of data for evidence gathering. The experimental results show that the Fuzzy agent IDS is more effective than the current IDSs. The proposed architecture allows local analysis and sharing of results and as well as minimizing the communication costs, The only disadvantage of this approach is the existence of a control center carrying out the major part of the intrusion detection.

By presenting a multi-level agent-based intrusion detection system, [14] showed that applying agent-based technology to intrusion detection system provides effective malicious detection; the system was able to detect most of the intrusive events. The experimental results have shown that agent-based technology is an efficient tool for building intrusion detection system infrastructure. Although the system faces some shortcomings such as the detection process is slow, the effective detection of autonomous attacks is still very low. Another major problem is protecting the security system from attacks, since the role of IDS is to monitor and ensure security of the protected system, the IDS itself is primary target of the attacks.

In his work, [15] presented an agent-based intrusion detection system based on misuse detection. He outlines the use of agent technology in intrusion detection which has practical advantages. The evaluation results show that agent intrusion detection systems do not only perform better in terms of effectiveness but also in terms of detection delay. The major drawback of the work is the inability to detect novel attacks, new threat which does not have signatures yet.

IV. PROPOSED SOLUTION

In order to overcome the limitations in the existing intrusion prevention system, we propose an anomaly prevention system based on risk analysis and inspired by the human nervous system. As in the nervous system, the proposed anomaly prevention system uses small, autonomous, and intelligent intrusion detectors as sensors as illustrated in Figure 1. The intrusion prevention system is situated inside the host and monitors its resources *(such as application activities, system calls, file access and modifications, etc)* for suspicious activities.

The role of the nerves like intrusion prevention is to manage these autonomous agents by providing them a high-level control commands such as indication to start or stop execution or to change some operating parameters from other entities, and to provide a set of prevention rules that will attempt to stop the attack before it happens. Since agents are independently-running entities, they can be added and removed from the protected system without altering or affecting other components, and without having to restart the intrusion prevention system. Furthermore agents may provide mechanisms for reconfiguring them at runtime without even having to restart them to achieve the continuous running with minimum human intervention. Additionally, an agent may also be part of a group that can perform different functions but also can exchange information and derive more complex results that any one of them may be able to obtain on their own.

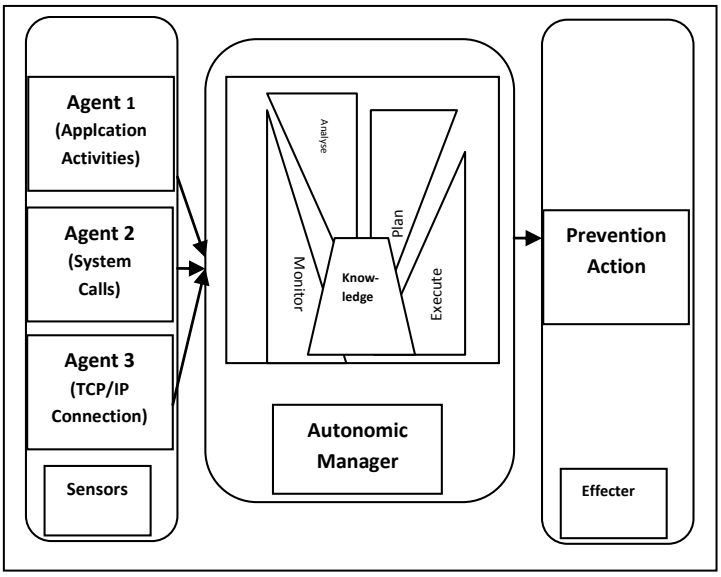

Figure 1: Agent-based Autonomic Intrusion Detection and Prevention System

V. DISCUSSION

In the proposed intrusion detection and prevention system, data collection and analysis elements are operated by autonomous agents based on risk assessment and managed on the basis of the autonomic computing theory with self-management properties. This approach solves most of the limitations of current intrusion detection and prevention systems more effectively with minimum human intervention. The main purpose of using autonomic computing is to create computing systems capable of managing themselves to a far greater extent when given high-level objectives, and to provide set of prevention rules that will attempt to stop the attack before it happens depending on risk analysis and risk assessment. These will help to confirm the validity of the alerts and identify the false positive alerts, by measuring the risk caused by the detected threat, in order to determine whether it is a normal activity or not. To accomplish the desired features, the proposed autonomic management model will be categorized into six levels as depicted in Figure 2.

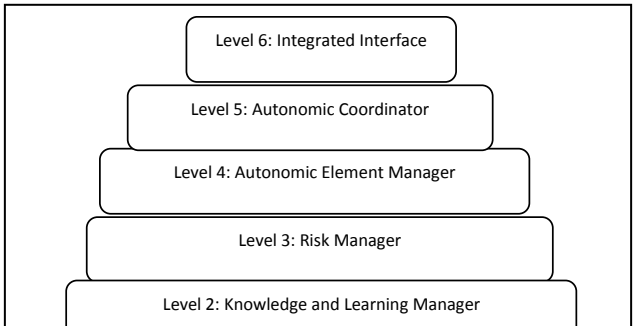

Figure 2: Levels of Administration in the Agent-based Autonomic Intrusion Detection and Prevention System

Each level carries out specific services. The top of the pyramid (Level 6) addresses the integrated autonomic interface. This interface is the unique contact point of the user with the autonomic architecture. This is the place where strategies and policies are defined by the user. At the base (Level 1) the operational manager manages a number of autonomous agents (intrusion detectors) which in turn monitors system resources for existence of incidents. The middle of the pyramid (Layers 2, 3, 4 and 5) addresses the knowledge and learning manager that controls all the knowledge repositories and the deduction module; the risk manager that evaluate and analyse the risk of the detected threat according to strategies and guidelines provided by system administrator through Layer 6; the autonomic elements manager that manages each autonomic component (self-configuration, self-optimization, self-healing, and self-protection) individually; and the autonomic coordinator that harmonizes all the autonomic components together.

VI. CONCLUSIONS AND FUTURE WORKS

Findings from our studies indicate that existing intrusion detection and prevention systems have some limitations and drawbacks. Hence, the need to deploy distributed autonomous agents based on autonomic principles. Autonomous software can act independently from one another and perform different tasks in a collaborative manner. Self configuring is responsible for ensuring overall system management is coordinated and synchronized by these agents.

Furthermore, since agents behave independently, also reconfiguration of sensors is usually difficult but through collaboration and coordination management it can be simplified and made effective. In this paper we proposed a solution that is more effective than current intrusion detection and prevention systems. The proposed solution offers an intelligent fault tolerant self-managed intrusion prevention system with continuous runtime and minimum human intervention due to the use of multi-agents supervised by autonomic manager, with minimum number of false-positive alarms due to the use of risk analysis and risk assessment. With the self-management properties the system can dynamically adapt to changing environments, monitor and tune resources automatically, discover, diagnose and react to disruptions automatically.

Future works in this area could be to monitor not only the host resources but also the entire network by distributing these agents in a roving manner to make network-based intrusion prevention system to deliver maximum security by anticipating threats as and when they happen. Another possible future work could geared towards implementing it with the use of mobile agents which have the capabilities to autonomously incarnate, migrate and consolidate inside the network from host to host to detect intrusions and execute prevention as a total solution against all known and some unknown generic threats.

REFERENCES

[1] R. Heady, G. Luger, A. Maccabe and M. Servilla “The architecture of a network level intrusion detection system”Technical Report, Computer Science Department, University of New Mexico, August 1990.

[2] Martin, Chris. "What Is IPS and How Intrusion Prevention System Works." aboutonlinetips.com, 2009.

[3] “NIST- Guide to Intrusion Detection and Prevention Systems (IDPS)”. 2007-02 [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf. Retrieved 2010-06-25.

[4] Robert C. Newman (19 February 2009). *Computer Security: Protecting Digital Resources*. Jones & Bartlett Learning. pp. 273–. ISBN 9780763759940. http://books.google.com/books?id=RgSBGXKXuzsC&pg=PA273. Retrieved 25 June 2010.

[5] Michael E. Whitman; Herbert J. Mattord (2009). *Principles of Information Security*. Cengage Learning EMEA. pp. 289–. ISBN 9781423901778. http://books.google.com/books?id=gPonBssSm0kC&pg=PA289. Retrieved 25 June 2010.

[6] Zhou, Ping, and Jian Fang. "Intrusion Detection Model Based on Hierarchical Fuzzy InferenceSystem." In Second International Conference on Information and Computing Science, 144-47: IEEE Computer Society Press, 2009.

[7] Tim Boyles (2010). *CCNA Security Study Guide: Exam 640-553*. John Wiley and Sons. pp. 249–. ISBN 9780470527672. http://books.google.com/books?id=AHzAcvHWbx4C&pg=PA249. Retrieved 29 June 2010.

[8] Harold F. Tipton; Micki Krause (2007). *Information Security Management Handbook*. CRC Press. pp. 1000–. ISBN 9781420013580. http://books.google.com/books?id=B0Lwc6ZEQhcC&pg=PA1000. Retrieved 29 June 2010.

[9] "NIST - Guide to Intrusion Detection and Prevention Systems (IDPS)". 2007-02. http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf. Retrieved 2010-06-25.

[10] John R. Vacca (2010). *Managing Information Security*. Syngress. pp. 137–.ISBN 9781597495332. http://books.google.com/books?id=uwKkb-kpmksC&pg=PA137. Retrieved 29 June 2010.

[11] Engin Kirda; Somesh Jha; Davide Balzarotti (2009). Recent Advances in Intrusion Detection: 12th International Symposium, RAID 2009, Saint-Malo, France, September 23-25, 2009, Proceedings. Springer. pp. 162–.ISBN9783642043413. http://books.google.com/books?id=DVuQbKQM3UwC&pg=PA162. Retrieved 29 June 2010.

[12] F Xu, Xin, Zunguo Huang, and Lei Xuan. "Autonomic Computing for Defence-in-Depth Information Assurance: Architecture and a Case Study." Springer-Verlag Heidelberg (2004).

[13] Wasniowski, R. A. (2005) Multi-sensor agent-based intrusion detection system. Information security curriculum development. Kennesaw, Georgia ACM.

[14] Sodiya, A. S. (2006) Multi-level and Secured Agent-based Intrusion Detection System. Journal of Computing and Information Technology, 14, 217-223.

[15] Barika, F., Kadhi, N. E. & Ghédira, K. (2009) Agent IDS based on Misuse Approach. Journal of Software, 4, 495-507.

[16] Barika, F., Kadhi, N. E. & Ghédira, K. (2009) Agent IDS based on Misuse