International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-2 Number-4 Issue-6 December-2012

Distributed Approach of Intrusion Detection System: Survey

Vineet Richariya[1], Uday Pratap Singh[2], Renu Mishra[3]
Computer Science & Engineering, LNCT, Bhopal, India

Abstract

Intrusion Detection Systems (IDS) are now becoming one of burning issue for any organization's network. Intruders always search for vulnerabilities or flaws in target system and attack using different techniques. An intrusion detection system (IDS) is needed to detect and respond effectively whenever the confidentiality, integrity, and availability of computer resources are under attack. Today, number of open sources and commercial Intrusion Detection Systems are available to match organization's requirements but the performance of these Intrusion Detection Systems is still the main concern. In this paper, we have analyzed the performance and applicability of the well knows IDS system based on mobile agent with their pros and cons. Mobile agent is efficient way to find out the intruder in distributed system. The main features of mobile agents are intelligence and mobility which is the core motivation to us to designed cost. The aim of this review work is to help to select appropriate IDS systems as per their requirement and application.

Keywords

Intrusion-Detection, Mobile Agents, Network Security.

1. Introduction

With the thriving technology and the great increase in the usage of computer networks, the risk of having these networks to be under attacks having been increased [2]. There is currently a need for an up-to-date, thorough taxonomy and survey of the intrusion detection [8]. This paper presents such taxonomy, together with a survey of the important research intrusion detection systems and a classification of these systems according to the taxonomy. Significant the main focus of this survey is intrusion detection systems through mobile agent and its limitation [14, 5]. Now a day's intrusion detection with web log file is hot and burning issue. It has been seen in previous work that IDS with web log files are very flexible, efficient and scalable [13]. Log file is a simple plain text file which record information about each user access. Log file contain information about user ID, IP address, date, time, bytes transferred, access request. A Web log is a file to which the Web server writes information each time a user requests a resource from that particular site. When user submit request to a web server that activity are recorded in web log file. Log file range 1KB to 100MB. Web log file is located in three different location Web server logs, Web proxy server, and Client browser [22, 13].

The major challenges and requirements for building intrusion detection systems are:

1. Ability to detect attacks reliably without giving false alarms. The challenge is to build a system which can detect a wide variety of attacks and at the same time which results in very few false alarms.
2. Ability to handle large amount of data without affecting performance and without dropping data. The challenge is to prevent an attack rather than simply detecting it.
3. Ability to link an alert generated by the intrusion detector to the actual security incident is desirable. It is not only necessary to detect an attack, but it is also important to identify the type of attack.

Mobile agents are designed for remote access or computation of data It reduces network traffic through perform data computation at remote/client side [17]. This characteristic make mobile agent best suitable in IDS system. Working of mobile agent is much like Remote procedure call (RPC), Remote method invocation [RMI] and .NET Remoting [18]. Its often create confusion concept of cloud computing with mobile agent because they are similar in a way that they work on loosely coupled distributed environment. Cloud is designed for resource sharing and mobile agent for remote computation [32].

2. Intrusion Detection System (IDS)

Basically, there are two possibilities to secure an organizational network against intruders. First is to build complete secure network system by applying all complicated cryptographic, authentication and authorization methods. However, this solution is not

realistic [4]. In practice, it is impossible to have completely secure system, because the user uses operating system and other applications to accomplish his/her job. Almost all applications have one or the other vulnerabilities. Second way is to detect an attack as soon as possible preferably in real-time and take appropriate action. This is essentially what an Intrusion Detection and Prevention System (IDS and IPS) does [19].

Intrusion means to interrupt someone without permission. Intrusion is an attempted act of using computer system resources without privileges, causing incidental damage. Intrusion Detection means any mechanism which detects the intrusive behavior. Intrusion Detection System (IDS) from the name itself, people could interpret that an IDS is a system used to monitors network traffic and detect its suspicious behavior against security. If it detects any threat then alerts the system or network administrator. The objective of IDS is to detect and inform about intrusions. IDS is a set of techniques and methods that are used to detect suspicious activities both at the network and host level [20].Intrusion detection systems (IDSs) are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems [11].

The desirable characteristics for IDS are following:

- Run continuously without human supervision,
- Be fault tolerant and survivable,
- Resist subversion,
- Impose minimal overhead,
- Observe deviations from normal behavior,
- Be easily tailored to a specific network,
- Adapt to changes over time

3. MA-IDS Architecture

Mobile agents offer unique features that can be used to improve the ways in which IDS are designed, developed and deployed in the network [9]. IDS implemented using mobile agent is one of new paradigms for intrusion detection. MAs are particular software agents having the capability to move from one host to another. The software agent can be treated as Mobile Agent [22], as they are able to migrate from one computer to another computer. Even if the host machine, which launched the agent, is eliminated from the network, the agent can still work.

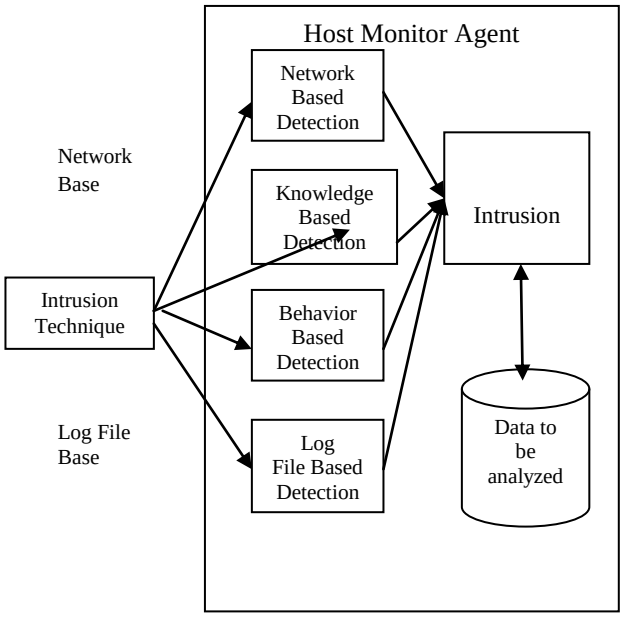

Figure 1: Host Monitor Agent Structure

Thus, the mobile agents are very powerful programs, which can act even in the absence of the machine that initiated them [7, 3]. After completion of their assigned tasks, the mobile agents return to the host machine to report the result or simply terminate.

The platform where a mobile agent originates is referred to as the home platform (controlling device), and normally is the most trusted environment for an agent [17]. One or more hosts may have an agent platform, and an agent platform may support multiple locations or meeting places where agents can interact.). Figure 1 shows that mobile agent gathered data and send back to the controlling. Figure 1 shows the working of host mobile agent.

4. Distributed Approaches

1. A Novel Network Attack Audit System based on Multi-Agent Technology

They proposed [21] a network attack audit system which includes network attack audit Agent, host audit Agent and management control centre. The audit system in terms of network attack is just in-depth, and with the function improvement of network attack audit Agent, different attack will be better analyzed and audit. In addition, the management control centre Agent should manage and analyze audit results from AA (or HA) and audit data on time. And the history files of network packets and host log data should also

be audit to find deeper violations that cannot be found in real time. A local area network security audit model was presented based on multi-agent, and proposes an improved information entropy detection algorithm can obtain audit modules. In practice, the audit system can effectively improve the auditing efficiency, intelligence logging data analysis.

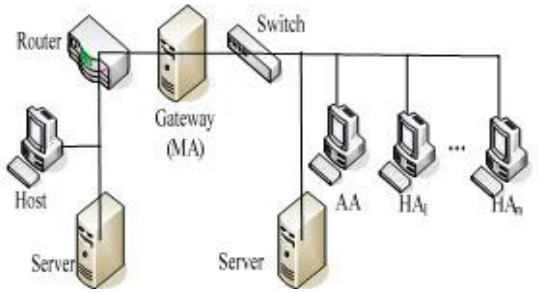

Figure 2. Network distribution chart of Multi-Agent network security

System Model

According to the properties of Agent, in LAN, security audit system can be separated into three parts: network attack audit Agent (AA), host audit Agent (HA) and management control center Agent (MCA), network distribution is shown as Figure 2. Different methods are used to achieve different functional Agents, the details are as follows:

1) Reducing the waste of resources in LAN

Agent technology is used to collect and audit all sorts of logging data in different hosts, can avoid the logging data into a single server to lighten the burden of server in order to reduce the waste of bandwidth or other network resources.

2) Improving audit efficiency.

Different host agent can be specified to different nodes auditing tasks backbone or key point, close to the server. Audit methods according to reasonable use drug audit task, for example, association rule mining algorithm can be used to audit host operating actions, improved information entropy algorithm can be used in network audit proxy detection DDoS attack, and all of these can improve efficiency of the whole audit system.

2. An Efficient Formal Framework for Intrusion Detection Systems

Traffic anomalies and attacks are commonplace in today's networks, and identifying them rapidly and accurately is critical for large network operators [10]. Intrusion detection systems are an important component of defensive measures protecting computer systems and networks from abuse. For an intrusion detection system, it is important to detect previously known attacks with high accuracy. However, detecting previously unseen attacks is equally important in order to minimize the losses as a result of a successful intrusion. It is also equally important to detect attacks at an early stage in order to minimize their impact. To address these challenges, they proposed to improve the efficiency of the network intrusion detection process by including an Event Calculus based specification to detect the registered and expected behaviour of the whole network. The detection model consists of the following elements:

Security Requirements: define properties that should be satisfied to guarantee the security of the network.

Assumptions: are additional properties injected to facilitate the verification process. Security properties that wit is not sure of and more important, properties that cannot be efficiently monitored will be declared as assumptions.

Network specification: gives an abstract model for security critical entities of the network. One way to develop a specification for a program is to first identify what operations and accesses the program needs to support its functionality.

IDS rules: vary dependent on the IDS. In our case, they focused on Snort rules. Little research has been done on analyzing intrusion-detection rules.

Event logs: are necessary for the model because almost all IDSs are based on the analysis of the audit trails from operating systems, applications and network components.

3. Performance Evaluation Study of Intrusion Detection Systems

They have tested and analyzed the performance of the well know IDS system Snort and the new coming IDS system Suricata [1].Both Snort and Suricata were implemented on three different platforms (ESXi virtual server, Linux 2.6 and FreeBSD) to simulate a real environment. Finally, a comparison of the performance of the two IDS systems is provided along with some recommendations as to what and when will be the ideal environment for Snort and Suricata. Snort is open source network intrusion prevention and detection system (IDS/IPS) that combines the benefits of signature, protocol, and anomaly based inspection. It uses set of rules to check for hostile packets in the network and then

generate alerts to the network administrator. The main aim of Snort, Suricata and any other IDS system is to effectively analyze all packets passing throw the network without any packet drops. Suricata is a rule-based Intrusion Detection/Prevention System (IDS/IPS) that takes advantage of externally developed rule sets to monitor sniffed network traffic and provide alerts when suspicious events take place. Like most IDS it is designed to fit within existing network security components. The summary of analysis is as below:

(i)It is worth pointing out that Snort proved to be performing best on FreeBSD as no packet drops were recorded up to this speed.

(ii)The differences in performance started at speeds of 1.5Gbps and above, were the number of packet drops has decreased specially on Snort.

(iii)It can be said that Snort is capable of handling packets of size 1470 well better than Suricata. Snort started dropping packets at the high speed of 1.0Gbps on virtual Linux but did not exceed 1.15% at the speed of 2.0Gbps.

(iv)Attack detection rate (Alerts)

During the evaluation, attacks have been generated to evaluate the performance of both IDSs in a heavy and mixed traffic. The initial test was performed with background traffic only. This was done to confirm that both Suricata and Snort are configured to generate the same number of alerts. We then went on generating the same attacks for both Snort and Suricata in high speeds network. The results are presented in Table 1.

Table 1: Comparison

Speed	Snort	Suricata
1.0 Gbps	100%	98%
1.5 Gbps	100%	91.8%
2.0 Gbps	99.7%	66.8%

4. Misconfigurations Discovery between Distributed Security Components Using the Mobile Agent Approach

In this work [6], author's present mobile agent based architecture to detect misconfigurations between these distributed components and generate a new set of rules free of errors. The proposed approach is based on the similarity between the parameters of a filtering rule and those of an alerting rule. The idea is to check these misconfigurations using the mobile agent approach that has proven its effectiveness in distributed applications. The proposed approach has several advantages:

Generation of a new set of rules: While applying intra-anomalies detection algorithm, the new set of generated rules are totally disjoints i.e., the order of rules is no longer relevant.

Adaptable architecture: Based on dynamic architecture, the proposed model is updated automatically when a new security component is added.

Optimization in the detection process: The proposed approach uses digital signatures to identify components whose rules have changed since the last intra-anomalies detection. This allows minimizing the number of components to be verified.

Exploitation of distributed architecture advantages: The use of the mobile agent approach alleviates tasks to be executed by the administrator in a centralized architecture and optimizes the bandwidth use.

5. IDS Challenges

Some shortcomings are inherent when IDSs are constructed [7, 15]. The most common shortcomings include the following items

Lack of Efficiency

IDSs are often required to evaluate events in real time. This requirement is difficult to meet when faced with a very large number of events as is typical in today's networks.

High Number of False Positives

Most IDSs detect attacks throughout an enterprise by analyzing information from a single host, a single application, or a single network interface, at many locations throughout the network. False alarms are high and attack recognition is not perfect.

Burdensome Maintenance

The configuration and maintenance of intrusion detection systems often requires special knowledge and substantial effort.

Limited Flexibility

Intrusion detection systems have typically been written for a specific environment and have proved difficult to use in other environments that may have similar policies and concerns. The detection mechanism can also be difficult to adapt to different patterns of usage.

End-to-end Encryption

With security improvements in communications protocols, the ability to encrypt traffic on an end-to-end basis is on the rise.

High Speed Communications

Higher communication traffic rates directly affect the processing speed needed to analyze packet content, potentially resulting in lost packets.

Breadth of Attacks

As new attacks are conceived, IDSs must be updated to discover them. While new attacks are added frequently, old ones can seldom be dropped.

6. Conclusions

In this work we have studied and reviewed some existing distributed based approaches for intrusion detection system. Various intrusion detection techniques are discussed in this paper to support the security of an organization against unwanted threats or attacks. Most of the existing intrusion detection systems are very straightforward. We focus upon the different type of intrusion detection system (IDS) approach like configuration detection Anomaly detection, Misuse detection, data mining etc. We have included the further challenges of reliable intrusion detection system. The IDS approach can be enhanced by providing more security to mobile agents. In future work there is need to investigate the new concept of behaviour to make this agent more intelligent to enhance the actual performance and track any new type of attack which is the main purpose to use the network IDS.

References

[1] Adeeb Alhomoud, Rashid Munir & Jules Pagna, "Performance Evaluation Study of Intrusion Detection Systems" The 2nd International Conference on Ambient Systems, Networks and Technologies (ANT), Science Direct 2011.

[2] Bhushan Trivedi , Jayant Rajput , Chintan Dwivedi and Pinky Jobanputra, "Distributed Intrusion Detection System using Mobile Agents ", IACSIT Press, Singapore 2011.

[3] Chris Peterson, "An Introduction to Network and Host Based Intrusion Detection Using Fuzzy Logic" IJCSE,2011.

[4] Dimitrios Damopoulos, Sofia A. Menesidou, Georgios Kambourakis, Maria Papadaki2, Nathan Clarke and Stefanos Gritzalis , "Evaluation of Anomaly-Based IDS for Mobile Devices Using Machine Learning Classifiers " , 2011.

[5] Damiano Bolzoni, Sandro Etalle, Pieter Hartel,"POSEIDON: a 2-tier Anomaly-based Network Intrusion Detection System, 2006 IEEE.

[6] Fakher Ben Ftima and Kamel Karoui, "Misconfigurations discovery between distributed security components using the mobile agent approach" 11th International Conference on Information Integration and Web-based Applications & Services, ACM 2009.

[7] Harley Kozushko, "Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems", September 11, 2003.

[8] Herve Debar, Marc Dacier , Andreas Wespi, "Towards a taxonomy of intrusion-detection systems" , 1999.

[9] Hakan Albag, "Network & Agent Based Intrusion Detection Systems ", TU Munich Dep. of Computer Science, Istanbul Tecical. University.

[10] Mohsen Rouacheda and Hassen Sallay, "An Efficient Formal Framework for Intrusion Detection Systems" The 2nd International Symposium on Frontiers in Ambient and Mobile Systems (FAMS), Science Direct 2012.

[11] Mahbod Tavallaee, Natalia Stakhanova, and Ali Akbar Ghorbani," Toward Credible Evaluation of Anomaly-Based Intrusion-Detection Methods", IEEE September 2010.

[12] Nisha Verma, Dr. Mohd Husain, Manoj Kumar Shukla, "Research on Mobile agent based network intrusion", June 2011.

[13] Roger Meyer, "Detecting Attacks on Web Applications from Log Files", 26 January 2008

[14] Manmeet Singh, S S Sodhi, "Distributed Intrusion Detection using Aglet Mobile Agent Technology ", March 23, 2007.

[15] R. Tiwari and R. Gour, "Mobile Agent Based Distributed Intrusion Detection System: A Survey" International Journal of Computer Applications in Engineering Sciences, September 2012.

[16] Syurahbil, Noraziah Ahmad, M. Fadly Zolkipli,Ahmed N. Abdalla," Intrusion Preventing System using Intrusion Detection System Decision Tree Data Mining", 2009 Science Publications.

[17] Vivek Tiwari, Dr. S.K. Lenka &Shailendra G.," Performance Evolution of Java Remote Method Invocation and Mobile Agent Techniques in Context of Distributed Environment" IEEE International Conference on Networking and Information Technology (ICNIT 2010) Manila.

[18] Vivek Tiwari & Shailendra G." Computational Study of .NET Remoting and Mobile Agent in Distributed Environment" International Journal of Computing, Volume 2, Issue 6, June-2010, ISSN: 2151-9617.

[19] Vivek Tiwari & Umesh Bindal,", Cloud Computing: A next generation revolution in IT with e –Governance" CiiT International Journal of Networking and Communication Engineering, Volume 2, DOI: NCE052012006, ISSN 0974-9616, May 2012.

[20] V. Jyothsna, V. V. Rama Prasad, K. Munivara Prasad, "A Review of Anomaly based Intrusion Detection Systems", August 2011.

[21] Wang Jianping, Chen Min & Wu Xianwen, "A Novel Network Attack Audit System based on Multi-Agent Technology" International conference on Solid State Devices and Materials Science, Science Direct 2012.
[22] Yongzhong Li, Rushan Wang, Jing Xu, "A Novel Distributed Intrusion Detection Model Based on Immune Mobile Agent " May 22-24, 2009.

Received her Master in Computer Application from M.P.C.T. Engineering college, Gwalior in 2007. She is currently M.Tech. (Soft. Engg.) scholar in L.N.C.T., Bhopal. She worked as Assistant Professor in Madhav Institute of Science & Technology (MITS) Gwalior. Her research interests in Network Security, Intrusion Detection system, soft computing.s.