ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

INTELLIGENT AGENTS FOR INTRUSION DETECTION SYSTEM (IAIDS)

K.Siva sankari, R.Dhivya bharathi
Computer Science and Engineering
Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College
Avadi, Chennai-600062.

Abstract

This paper presents a distributed wireless intrusion detection system (IDS) based on Intelligent agents. Intelligent agents are randomly traveled in difference nodes which are connected with the network. Each agent may perform specific tests (like mobile sensors). When the test indicates some possibility of an intrusion, the agent may ask for additional tests at the site. Only after the suspicion level has been raised too high, it triggers alarm to the security officer. Notice that the attack is confirmed by executing only relevant tests and the entire suite of tests does not have to remain resident at every node. The agents are traveled by means of random sampling method. The mobile agents themselves can also have statistical properties such as rate at which they test nodes, their size, the diversity of nodes visited etc., The proposed model comprises of four major components: Intrusion detection module, Alert, Mobile agent platform , Test suit.

***Keywords*—- Intelligent agent, Intrusion detection module, and test suit.**

I. INTRODUCTION

Wireless has opened a new and exciting world for many of us. However wireless networking are vulnerable in ways (eavesdropping, illegal use, Mac spoofing, monkey jacks, null probes, flooding attempts etc.,). In this paper we proposed WIDS (wireless Intrusion Detection system) based on client based Intelligent agents. It includes self learning, autonomy and self decision and self alerting.

This is multidimensional system in development which is intended to cover most of wireless networks specific vulnerabilities on intrusion. Among all security issues, intrusion is most critical and widespread. An Intrusion occurs when an attacker takes advantage of security vulnerabilities and thus violates the confidentiality, integrity or availability of the objects on the network. The fundamental approaches in intrusion detection system.

- Prevention: design, implement and configure the system as correctly as possible,
- Dissuasion: devaluate the system by camouflage or overestimate his protection,
- Detection: analyze the log file searching an intrusion signature or an abnormal behavior,
- Deflection: make the intruder believe that his intrusion is a success, while being diverted to a controlled environment,
- Correction: react when the intrusion takes place.

II. DEFINITION

Intrusion detection system (IDS) is a security system that monitors the computer and network traffic and analyzes that traffic for possible hostile attacks originating from outside the organization and also for system misuse or attack originating from inside the organization.

An intrusion is a deliberate, unauthorized attempt to access or manipulate information or system and render them unreliable or unusable. To be more precise when suspicious activity is from your internal network it can also be classified as misuse.

In the process of IDS there are two major contradictions may have a chances to occur, false negative and false positive. False negative are riskier than false positive since if there wasn't an attack and IDS classified as suspicious activity is referred as false positive it is not much harm but if there was an attack and IDS doesn't detect it referred as false negative then it can be very disastrous.

The main function of IDS includes 1. Monitoring and analyzing both user and system activities.2.Analyzing system configuration and vulnerabilities 3. Assessing system and file integrity 4. Ability to recognize patterns typical of attacks 5. Analysis of abnormal activity patterns 6. Tracking user policy violation.

Internet security has become more serious issue for anyone connected to the net. Currently the intension of hacking is mainly focusing on E-Commerce sites.

The frequency of attacks probes, intrusion attempts is inversely proportional to the difficulty level required to perform such attacks.

It is very difficult to build such IDS system that delivers cent percentage performance and also very difficult robust real – time IDS systems. There are many artificial techniques has been enhanced to reduce the human effort required to build these system.

The IDS can be categorized depend upon the type of attack being performed with the host system. The main aspect of IDS is to alert the security officer IDS can be divided into three broad categories.

Anomaly detection model vs. Misuse detection model. Anomaly detection model uses recognition techniques for operation sequence. They look for deviation from normal behavior. However they are capable for recognizing novel attacks. Anomaly detection is carried out by application of results of various scientific methods. There are many methods are possibly implemented like Clustering analyzes, Artificial intelligence methods, scientific mathematical abstraction detection model tech etc. Misuse intrusion detection model uses signature or rule based detection by which it is very immune and capable of identifying new attacks. Here IDS analyzes and groups all the available information and compares with rule list. Rule list are attack signature given (defined) by IDS. If any new attack has identified then it will update on the rule list. The main drawback is if the security of rule list is compromised that will cause serious damage to the system.

Network based system vs. Host based system This two types of the system are classified depend upon the scope of the security level. Network intrusion detection system (NIDS) is an independent platform that identifies the intrusion by examining network traffic and monitors multiple hosts. It directly connected to hub or switch and configured for post mirroring or network tab. It has the sensors and placed at inbound and outbound access points, which could be network borders. Sensors will captures all the network traffic both inbound and outbound and analyze the content of individual packets for malicious traffic.

Host based intrusion detection system (HIDS) is setup to detect illegal activities with in the host. The host that identifies the intrusion by analyzing application logs, file system modification, password files, database log list, Access control list. Generally HIDS is a software agent that will audit the logs.

Passive system vs. Reactive system In the passive system IDS detect al the security violations and analyzes all the suspicious activities, create a log file and alert the security officer. The reactive system create a log file capture the user activities disconnect the user from network traffic even log off the user from the system.

Nutshell analysis of IDS system.

- Signature based (Pattern matching)
- Statistical based.
- Integrity Checker
- Anomaly Detection/Behavior Based
- Flow Based

Basic types of response of IDS system

- Alteration to the environment
- Striking back (not recommended)
- Real time notification
- Throttling
- Session Sniping

III. Intelligent Agents Based IDS

Based on the distributed architecture, the proposed model integrates the concept of distributed agents and mobile computing. Agent includes various entities that detect and take predefined actions against malicious activity. It could be implemented as software running on servers and host or as independent hardware devices segments.

To implement the mobile agent system under the above security principles, categorized the requirements into three aspects.

- Agent privacy and integrity.
- Agent and server authentication.
- Authorization and access control.

IV. Features Of Mobile Agents.

An agent is a physical or logical entity characterized by the following attributes.

Autonomy: agents are independently-running entities; they operate without the direct intervention of Humans or others.

Mobility: agents are able of suspending processing on one platform and moving to another, where they Resume execution of their code.

Rationality: agents embody the capacity to decompose and solve a problem in a rational manner.

Reactivity: agents perceive their environment and response in a timely fashion to changes that occur in it.

Inferential capability: agents are able to use prior knowledge of general goal in order to act on tasks.
Pro-activeness: agents can take the initiative to act and response to their environment.
Social ability: agents are able to meet and interact with other agents. The interaction and collaboration between agents is achieved by an agent communication language and may depend on ontology to realize a common understanding of a situation.

V. INTELLIGENT AGENT IDS FRAMEWORK

I. Intelligent -Agents Architecture

The Test suit is the engine component of our system. It must combine several kinds of attack analysis such as signature detection, anomaly detection and performed global analysis, for detecting distributed attacks. Due to the complex analyzing tasks, the Test suit delegates performed tasks to well defined agents and uses different data sources. As shown in figure 1, it delegates predetermined performed tasks to four agents (Filter, Analyzer, Correlate, Interpreter and Mobile).

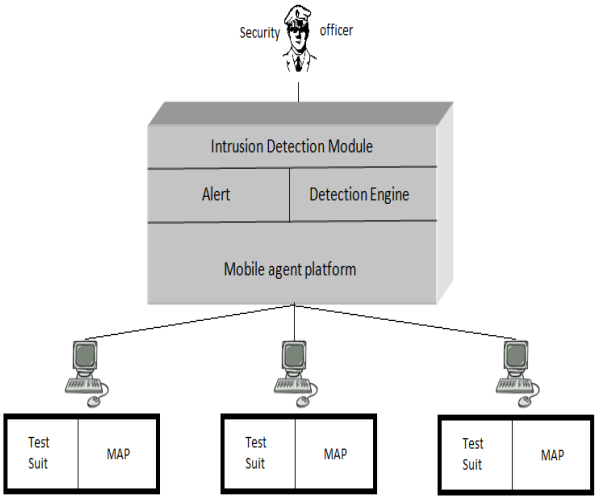

Fig: 1 Architectural view of Intelligent agents

II. Agent migration (Intelligent agents)

Agent migration will cause agent mobility and portability issues. Portability is generally solved by JVM (Java virtual machine). According to what need to be transferred and who initialized the mobility, agent mobility can be categorized into different degrees, such as remote execution, code on demand, and strong migration. In Remote Execution, the agent program is transferred before its activation to some remote node, where it runs until its termination.

The information transferred includes the agent code plus a set of parameters. In Code on Demand, the destination itself initiates the transfer of the program code. Both Remote Execution and Code on Demand support only code mobility because both schemes transfer agent programs before their activation. The standard agent mobility means migrating agents with not only code but also the state to the destination. The highest degree of mobility is Strong Migration. In this scheme, the underlying system captures the entire agent state (consisting of data and execution state) and transfers it together with the code to the next location. It requires a global model of agent state as well as the transfer syntax for this information.

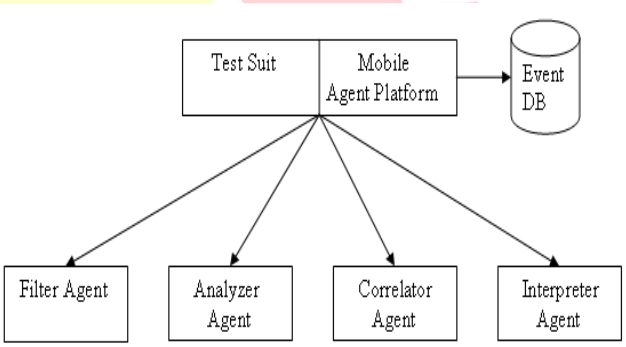

Fig: 2 Components of individual Intelligent agent

III. Flow Data Source

In the high design level, suspicious network traffic is captured by Snort sensor and log files are generated. SNORT is an open source NIDS. It is able to perform the analysis of network traffic in a real-time using a rule-driven language, which combines the benefits of signature, protocol and anomaly based inspection methods [16]. In fact, Snort is primarily a rule-based IDS, however input plug-ins are present to detect anomalies in protocol headers [17]. This NIDS is usually used to detect various attacks such as port scan, buffer overflow, web applications attacks and virus attacks. SNORT has three basic components:

- Packet capture: Sniff and collect network event,
- Rule matching: comparative analysis between the collected event and the attack signature,
- Output: the generated result from the rule matching.

An example rule is :
Alerttcp $EXTERNAL_NET any- $HOME_NET 21
(msg:"FTP passwd attempt"
flags:A+; content:"passwd";)

The rule header consists of the action keyword alert and everything else before the left parenthesis, and the parenthesized list contains the rule options. This rule matches TCP packets from any external source IP address and port, to port 21 on the local network, containing the string passwd and having at least the ACK flag set. Whenever a matching packet is found, an alert is generated with the text"FTP passwd attempt". SNORT has three different modes:

- *Sniffer mode*: read all network packets and display them into its interface,
- *Audit mode*: save the network event on the log file,
- *Detection intrusion mode*: analyze the network traffic, compare it with the intrusion signatures and perform actions accordingly.

According to event keywords specified in intrusion detection module, *Filter Agent* is agent responsible for filtering specialized security events from the log files. It examines the packets for well-known attack events and stores all its characteristics into *Event DB*. According to events rules, we have identified two event types: local events occur in a local network node and extern events occur in other network nodes. Specialized Local Agent delegates the filtering tasks to different *Filter Agents.*

IV. Intrusion detection module

Intrusion detection module contains no of events rules, it is an indication of intrusion. A security event is characterized by its signature, its type, location, and a temporal attribute representing the event occurring moment. According to the event type and its observation point, identifies various events classes. In our model, each event is characterized also by its keyword signature attacks, for example ping, nmap, etc. Based on the combination of keyword signature events, a set of a set of attack rules has been defined for well-known attacks. A rule is a set of requirements that will trigger an alert. Each rule is characterized by its sequence of events and the alerts block describing the predetermined actions executed by the system where an events has been occurred. We have identified two classes of signature rules:
- Local event rules, where all events occur in the same network node:

(1) Alert <actions> when even_local1, ...,even_localn

- Extern event rules, where at least one event of the given sequence events rule occurs in other local network nodes. This class of event rules is introduced to detect distributed attacks:

(2) Alert <actions> when even_local1, ...,even_localn and then even_ext1 ,...even_extm.

V. Intrusion Detection Module

The heart of our detection mechanism is the *Interpreter Agent.* It collaborates with the *Analyzer Agent* for detecting complex local attacks, and uses the *Correlate agent* with the *Mobile Agent* for determining whether some suspicious activities in different node can be combined to be a distributed intrusion. According to local event rules, the analyzer agent is responsible for detecting local intrusions. The *Analyzer Agent analyses* the events database. It looks for the local events selected by the *Interpreter Agent*. These patterns are retrieved from *Events DB*. Then, it reports a search results to the *Interpreter Agent* using its Specialized Local Agent. It's clear that correlation of the relevant events significantly reduces the number of false positive and gives a better view of an attack scenario in case of coordinated distributed attacks According to extern event rules given by the *Interpreter Agent,* the correlate agent is responsible for determining whether some suspicious activities in different network nodes can be combined to be a distributed intrusion. It queries the events database to search the occurrence of some event, and accesses to database events to store the occurrence of the external event received from other network nodes using *Mobile Agent*. A mobile agent based IDS uses agents with analysis capabilities to perform remote query and search actions. In our IDS model, mobile agent is used to perform well defined tasks: search the events occurrence in a given network or confirm occurrence of some event in a local network node. In the case of correlating events for detecting distributed attacks, the mobile agent is used to confirm the occurrence of some event in network nodes. For example, if the intrusion detection module is informed by the correlate agent that some correlating events are detected in the local network area, it would dispatch a mobile agent to search the occurrence of the same event type in the network nodes, and report the responses in its results area. The other case is made where Intrusion detection module receive a mobile agent to confirm some extern event. Figure 2 shows the itinerary example taken by the mobile agent from node source to nodes 1 and 2. Mobile agent created by specialized agent of node source looks for confirming the *Event1* by nodes 1 and 2, and also informs them that the Event2 occurred. Fig. 2 Itinerary Example of a Mobile Agent the Interpreter Agent behavior can be seen as an inference engine system. It processes the events Knowledge encoded in the Knowledge base
(Intrusion detection module – Event rules) for detecting the attacks.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

It consults the Event Rules and repeats the following scenario:

- Choose the first rule with no active state
- Make this rule in active state
- Submit the local events belonging to the premise part of the given rule (1), to the Analyzer Agent that have the pattern matching task to confirm the occurrence of the given events in Event DB When all the local events of the given rule have been occurred, the Interpreter Agent makes the rule in not active state. And then transmits the alert actions to the Specialized Local Agent. In the case of the extern rule (2), the Interpreter Agent completes the pattern matching task by submitting the extern's events to the Mobile Agent. The extern event is characterized by its node location. The extern event locations give the itinerary taken by the mobile agent, and then it looks for confirming the given events. When all the local and extern events of the given rule have been occurred, the Interpreter Agent deactivates the rule. And then transmits the alert actions to the specialized local agent.

VI. CONCLUSIONS

In this paper, we have proposed an approach for distributed intrusion detection system based on the specialized Intelligent agent and the agents community concepts. A specialized Intelligent agent is used to separate monitoring tasks. The agents community is a group of specialized agents, created for collecting and analyzing all the data transit from all predetermined network nodes. The specialized local agent executes predetermined actions and uses the Mobile Agent Environment to investigate all the other network nodes of the same community. The agents community collaborate and cooperate for confirming intrusion in predetermined network.

Acknowledgement

I would like to thank my Guide ,HOD and Staff members of my department for their cooperation and encouragement towards us to develop this innovative idea.

REFERENCES

[1] G. Hulmer, J. S.K. Wong, V. Honavar, L. Miller, Y. Wang, "Lightweight Agents for Intrusion Detection", Journal of Systems and Software

[2] W. A. Jansen, "Intrusion detection with mobile agents", Computer communication

[3] C. Kruegel and T. Toth "Applying Mobile Agent Technology to Intrusion Detection", technical report, University of Vienna, TUV-1841-2002-31, 2002.

[4] S. Fenet and S. Hassas, "A Distributed Intrusion Response System Based on Mobile Autonomous Agents Using Social Insects Communication Paradigm". Published by Elsevier Science B. V.,

[5] K. Singh, Son Vuong "Blaze: A Mobile Agent Paradigm for VOIP Intrusion Detection System", Proceeding of ICETE 2004, First International Conference on Business and Telecommunication Networks, Setubal, Portugal, August 2004.

[6] M. Roesch, "Snort: Lightweight Intrusion detection for networks", A white paper on the design features of snort 2.0, 2004.

[7] Wayne Jansen, Peter Mell, Tom Karygiannis, Don Marks. "Applying Mobile Agents to Intrusion Detection and Response". NIST Interim Report (IR) October 1999.

[8] D. E. Denning. "An intrusion-detection model". In proceeding of the IEEE Symposium on Security and Privacy, pages 118-131, April 1986.

[9] D. S. Bauer and M. E. Koblentz. NIDX – "an expert system for real-time network intrusion detection" In Proceeding of the Computer Networking Symposium, pages 98-106, Washington, DC, April 1988.

[10] Richard Feiertag, Sue Rho, Lee Benzinger, Stephen Wu, Timothy Redmond, Cui Zhang, Karl Levitt, Dave Peticolas, Mark Heckman, Stuart Staniford, and Joey McAlerney. "Intrusion detection inter-component adaptive negotiation". Computer Networks 34 (2000) 605-621.

[11] Mohammad Zulkernine -" DIDMA: A Distributed Intrusion Detection System Using Mobile Agents" proceedings of the Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallell Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Networks (SNPD/SA WN'05)

[12] G. White, E. Fisch, and U. Pooch, "Cooperating security managers: A peer-based intrusion detection system," IEEE Network, 1994.

IJARBEST
Research at its Best !!!