ISSN No. 0976-5697

Volume 2, No. 3, May-June 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Mobile Agent Applications within Intrusion Detection Technology

Nisha Verma*
Department of Computer Sc. & Engineering,
C-DAC,
Noida, India
nishaverma.access@gmail.com

Anjani kumar
Department of Computer Sc. & Engineering
C-DAC,
Noida, India
anjanikyadav@gmail.com

***Abstract*:** Intrusion detection system (IDS), based on mobile agents, that detects intrusion from outside the network segment as well as from inside. Mobile agent technology offers a new computing paradigm in which a program, in the form of a software agent, can suspend its execution on a host computer, transfer itself to another agent-enabled host on the network, and resume execution on the new host. As the sophistication of mobile software has increased over time, so too have the associated threats to security. This paper also researches the Agent technology and analyzes the characteristics and architecture of it. Finally this paper proposes the advantages and disadvantages to apply the mobile agent technology to intrusion detection systems, and points out the research direction of the intrusion detection systems based on mobile agent technology with their limitations.

Keywords: Information security; intrusion detection; mobile agent, MAP, IDS.

I. AGENT TECHNOLOGY

Agent is defined by the Agent-ISO FIPA (Foundation for Intelligent Physical Agent).Agent is a system with the following characteristics

- Agent lives in artificial world *S* together with other agents
- Agent can perceive and act in his environment
- Agent possesses a representation of the world *S*
- Agent is goal-oriented and can plan his actions and
- Agent can communicate with other agents

Agents are autonomous, persistent (software) components that perceive, reason, communicate and act in someone's favors, influencing its environment .in other words An agent is a software entity with a well-known identity, state and behavior, with autonomy to somehow represent its user . An *agent-based application* is a dynamic, potentially large-scale distributed application in an open and heterogeneous context such as the Internet. An agent can also defined that An agent is a computer system that is situated in some environment and that is capable of autonomous action in this environment in order to meet its design objectives; intelligent agent is autonomous, reactive, proactive and capable to communicate with other agents.

II. MOBILE AGENT INTRODUCTION

A. Mobile agent

Mobile agent is software code that can move from one computer to another computer with its execution state .In other words A mobile agent has the unique ability to transport itself from one system in a network to another in the same network. mobile intelligent entity, having specific function program segment, the program code independent of operating platform and system, so it can roam in the computer network and able to perform specific task .

The term "mobile agent" was introduced by Telescript, which supported mobility at the programming language level. In many ways, Telescript was ahead of time, including its support for mobile agents. Many mobile agent systems followed, most implemented in Java, which already supports mobile code, but also in scripting languages, such as Tcl/Tk or Python[1].Mobile agents seem suitable for applications, such as electronic commerce, system administration and management (especially network management), and information retrieval. However, few systems actually deployed them in an industrial setting. A mobile agent is contains

- Code
- Data State
- Execution State

Migrating Code = Mobile Code

Migrating Code + Data = Mobile Object

Migrating Code + Data + Execution State =Mobile Agent

Figure 1.Mobile agent

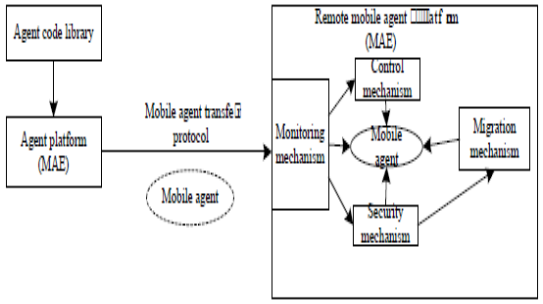

Figure 2. Mobile agent system architecture

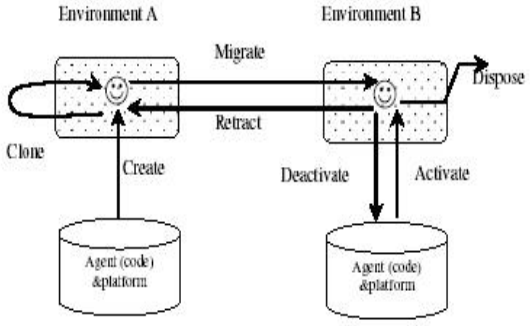

Figure 3. Mobile agent structure and life cycle

B. Mobile agent structure and life cycle

The life cycle of a mobile agent

1. The mobile agent is *created* in the Home Machine.
2. The mobile agent is *dispatched* to the Host Machine A for execution.
3. The agent executes on Host Machine A.
4. After execution the agent is *cloned* to create two copies. One copy is dispatched to Host Machine B and the other is dispatched to Host Machine C.
5. The cloned copies execute on their respective hosts.
6. After execution, Host Machine B and C send the mobile agent received by them back to the Home Machine [2].
7. The Home Machine *retracts* the agents and the data brought by the agents is analyzed. The agents are then *disposed*. From this we observe that a mobile agent experiences the following events in its life cycle:

Creation: A brand new agent is born and its state is initialized.
Dispatch: An agent travels to a new host.
Cloning: A twin agent is born and the current state of the original is duplicated in the clone.
Deactivation: An agent is put to sleep and its state is stored on a disk of the host.
Activation: A deactivated agent is brought back to life and its state is restored from disk.
Retraction: An agent is brought back from a remote host along with its state to the home machine.
Disposal: An agent is terminated and its state is lost forever.

III. MOBILE AGENT CHARACTERISTICS

(a)Intelligence

Software agents employ techniques from the field of artificial intelligence, which empower them with a fair degree of intelligence and common sense. For example, the travel agent program should realize that people generally do not prefer travelling by flights that depart or arrive at the airport late in the night and the agent should avoid booking tickets on such flights [3]. The travel agent program should be smart enough to bargain and arrange the trip so that the overall expenditure for the trip is as low as possible without compromising on the user's preferences.

(b)Autonomy

The agents themselves decide the sequence of actions to be performed to achieve the user's task. This autonomy enables agents to operate without requiring human intervention. Once the specifications are given to the travel agent, it should be able to proceed on its own to arrange the trip for the user without requiring the user to constantly monitor the agent.

(c)Responsiveness

Agents perceive their environment (which may be the Internet, a collection of other agents, etc.) and respond in a timely fashion to changes that occur in it. At the same time, agents should not simply act in response to their environment; they should be able to exhibit opportunistic, goal-oriented behavior and take the initiative when appropriate.

(c)Communicative Ability

Software agents should provide a user friendly interface so that the user can easily interact with the agent. Agents are social entities and often communicate and collaborate with one another in order to complete their tasks. For example, the travel agent program of one user must be able to communicate with other travel agents to find out about hotels which customers disliked and avoid such hotels.

(d)Adaptability

Mobile agents migrate from one computer to another in the network and execute on several machines. Mobility increases the functionality of the mobile Agents perceives their environment and responds in a timely fashion to changes that occur in it Agent allows the mobile agent to perform tasks beyond the scope of static agents.

(e) Platform-independent feature

Most of mobile agent uses the platform-independent language to make the program run on cross-platform. General mobile agent systems establish the platform-independent communication protocol matched with the mobile agents, through which it does need to establish a direct communication connection between the agents. In this manner it can be more easily to develop applications on heterogeneous platforms.

(f) Distribution flexibility

Mobile agent runs in the entire distributed system, rather than fixed at a particular location. In this way, once needed it can directly send itself or other needed mobile agents to the desired host site for local operation, which can improve the operational flexibility, while eliminate the dependence of the complex communication protocols of the traditional agent communication.

(g) Low-network data traffic

Mobile agent can filter the collected data, and then extract the key data. In this way, the data traffic through the network can be significantly reduced to improve the system overall availability.

(h) Strong fault tolerance

Mobile agent reduces the requirements of the network applications to the network connection reliability [4]. Mobile agent can automatically handle and correct its own mistakes to more easily build the distributed system with strong fault tolerance. For example, before a network node

is failure, the mobile agent works on it can immediately perceive complete the corresponding backup work, and then move to the other nodes continue to the original work.

IV.MOBILE AGENTS APPLICATION IN INTRUSION DETECTION

(i) IDS Requirements

We have categorized that set of desirable characteristics for an IDS system: functional and performance

1. Functional requirements
   - The IDS must continuously monitor and report intrusion
   - The IDS should have a very low false alarm rate
   - The IDS must provide enough information to repair the system in the case of intrusion detection
   - The IDS must detect and react to distributed and coordinated attacks. Coordinated attacks against a network will be able to marshal greater forces and launch many more and varied attacks against a single target.[5]
   - The IDS should be adaptive to network topology and configuration changes.
2. Performance requirements
   - Intrusion should be detected in real-time and reported immediately to minimize the damage to the network,
   - The IDS must be scalable to be able to handle the additional computational and communication load.

(ii)*Advantages of mobile agents applied to intrusion detection*

Mobile agent technology brings many advantages it can reduce network load, reduce network latency, asynchronous self-execution, dynamic adaptive, heterogeneous environment operation, robustness, & fault tolerance. The following will analyze the IDS-related advantages of mobile agent.

(a) Reducing network load and load balance

Mobile agent can distribute a larger calculation workload on multiple processors to avoid the emergence of bottlenecks and thus to achieve load balance.

(b) Overcoming network latency

Mobile agent can directly execute tasks on the nodes leaving the central control point to directly respond to a large number of events. In addition, the mobile agents are located in various parts of the network, so multiple routing can be selected to avoid the communication link failure.

(c) Executing Asynchronously & Autonomously

IDS architecture is coordinated by one or several central console (that is, a central controller), which needs reliable communication paths to be connected to the network sensor and intermediate processing nodes. Such key role of the central controller in the whole system makes itself become one of the main objectives to be attacked, failure probability is big. When a central controller failure or a communications link fails, the mobile agent still is able to continue working. Because that it is different with the message passing ,mobile agent sent from its home platform, regardless of its home platform existed, the network connection normal, the mobile agent are able to self-run.

(d) Adapting dynamically

The mobile agent can sense implementation environment changes and automatically respond to them mean they have property to adopting environment dynamically.

(e) Executing heterogeneous

Large enterprise network in general is composed by many different computing platforms and computing equipment, one of the greatest advantages of mobile agent is that it can achieve interaction operations at the application layer. Mobile agent can be independent of the calculation and the transmission layer, only depends on the execution environment to run, which provides an optimal solution for the seamless integration of heterogeneous systems [6]. In other words, as long as the installation of mobile agent platform, mobile agent can run on any network node in theory.

(f) Robustness and fault tolerance

Mobile agent the dynamic response capability to the external environment provides an advantage for the establishment of a high robustness, strong fault-tolerant systems. When a host shuts down, all the mobile agents implemented on it will be warned and left time, to make them preserve the existing implementation state to ensure the continuous operation when transferred to other hosts. The mobile agent support to the connectionless operation and distributed model eliminate the single point collapse problem, to provide a fault-tolerant feature for it. Thus it can be seen, in the field of intrusion detection, mobile agent technology has the advantages general technologies unmatched [7]. The purpose of this paper is to propose an intrusion detection model based on mobile agent technology and analyze it.

(iii) IDS limitations

The most common IDS shortcomings include the following:

- Higher number of false positive,
- Lack of efficiency: usually ,when an IDS is faced to a huge number of events in the network, it slow down a system or drop network packets that it don't have time to process[8].
- Vulnerability to be attacked: many IDS have hierarchical structures, this gives the opportunity to the attacker to harm the IDS by cutting off a control branch or even tacking out the root command

(iv) Disadvantages of mobile agents applied to intrusion detection

Although the introduction of mobile agent technology in IDS can bring about the above-mentioned advantages, but the developing technology will inevitably exist some issues. But we believe that these issues will be gradually overcome with the development of mobile agent technology.

(a) Security

In an open multi-agent system, agent can dynamically enter or leave the system, and it will interact with the agent platform and multiple agents, needed to be given certain

privileges (and sometimes the root user permissions) to complete its own tasks by using local resources. [9]Therefore, agent technology brings new security threats to the system, and these threats are: agent to agent, agent to platform, other entities to agent platform. So, how to ensure the security of systems and agent must be taken into account.

(b) Limited Exposure

The client-server computing paradigm is well understood and quite mature as a technology. An agent's envisioned autonomous behavior, involving collaboration with other agents at various network locations, creates a dynamic environment that requires new design methodologies and modeling tools to properly formulate and construct agent-based systems. The lack of mature agent design methodologies and modeling tools makes this task difficult, but the problem is likely to be overcome as commercial demand for these product increases and is eventually satisfied.

(c) Performance

The increase of the network bandwidth and the amount of detection data requires the IDS to quickly detect attacks and timely process the system events. And agent is usually achieved by slower explanatory language, and its implementation requires a virtual machine and interpreter support. Compared with the local code, the explanatory language may be difficult to meet performance requirements.

(d) Code size

IDSs are complex pieces of software. Agents that perform IDS services may thus be required to contain a large amount of code. If these agents are supposed to do operating system specific tasks on multiple operating systems then this code base may get extremely large. The size of MA code may limit the functionality of MAIDS because it will take a long time to transfer an agent between hosts.

(e) Coding and Deployment Difficulties

MAs' inherent capabilities, such as moving and cloning, add more complexity to the design and development process. Given this added complexity, MAIDS will be even more prone to faults than their non-MA counterparts. Further hampering near term MAIDS deployment is a lack of MA design, development, and management tools, needed before any large-scale deployment of agent-based applications becomes feasible. Agent developers and administrators could also benefit from better resource control mechanisms in MA platforms

V. MOBILE AGENT-BASED INTRUSION DETECTION SYSTEM RESEARCH

Mobile agent-based intrusion detection system is an implementation of the mobile agent approach in intrusion detection. According to the system designer, attackers follow four common steps to gain unprivileged access to remote machines. In the first step they scan for machines and ports, in the second stage they try to use vulnerabilities of common services. Following stage is the mark stage where the attacker gets actually access to the system and later in the masquerade stage they try to hide their actions by trying to erase logs, etc. Mobile agent-based intrusion detection system is aimed to detect intrusions by scanning marks left by the intruder, who is actually in the mark stage. The Mobile agent-based intrusion detection system has a simple structure, it consists of a central manager on each network segment, sensors and multiple kinds of agents, IDA (Intrusion detection agents) uses agents to collect information about the intrusion and the intruder, but the management is still centralized. From the preceding analysis of the advantages and disadvantages it can be seen, it significantly improved the IDS design, build, and implementation and operation methods. U.S. National Institute of Standards and Technology (KIST) gave and minutely analyzed the five major research directions of mobile agent in intrusion detection, which are IDS performance improvements, new intrusion detection model, existing architecture improvements, new architecture model, and IDS attack response.

6. CONCLUSION

This paper presents architecture and mobile agent life cycle for the development of an intrusion detection system based on mobile agents' .This paper introduced the mobile agent definition, and mobile agent characteristics, Applications of mobile agent in intrusion detection including the advantages and disadvantages of mobile agent technology applied in NIDS. From the analysis it can be seen that the application of mobile agents in assault technology has good effect.

V.REFERENCES

[1] Jai Bala subramaniyan, Jose Omar Garcia- Femandez, David Isacoff, etal, "An Architecture for Intrusion Detection using V6-552 *2010 2nd International Conference on Computer Engineering and Technology* [Volume 6]Autonomous Agents", Department of Computer Sciences, Purdue University; Coast TR98-05, 1998.

[2] V Paxson, Bro: A System for Detecting Network Intruders in Real-time,the Seventh USENIX Security Symposium, San Antonio, 1998.

[3] Joseph S.Sherif, Rod Ayers, Intrusion detection: methods and systems, Part II, Information Management & Computer Security, 2003.

[4] Eugene H. Spafford, Diego Zamboni, Intrusion detection using autonomous agents, Computer Networks, 2000,[Volume 6] *2010 2nd International Conference on Computer Engineering and Technology* V6-553.

[5] Wayne Jansen, Tom Karygiannis" Mobile Agent Security" National Institute of Standards and Technology Computer Security Division Gaithersburg.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] *Parineeth M Reddy* "Mobile Agents Intelligent Assistants on the Internet"general RESONANCE ,July 2002[7] Kornelije Rabuzin, Mirko Malekovi□, Miroslav Baca "A SURVEY OF THE PROPERTIES OF AGENTS" University of Zagreb, Faculty of Organization and Informatics, Varaždin 2006.

[8] Wayne Jansen, Peter Mell, Tom Karygiannis, Don Mark" Applying Mobile Agents to Intrusion Detection

and Response" National Institute of Standards and Technology Computer Security Division.

[9] Gao Kun , Jin Sumei "Research on the Application of Mobile Agent in Intrusion Detection Technology" Hebei academy of governance ,Information and Technology College, Hebei University of Economics and Business,2010.