Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Efficient use of Mobile Agents for Network Security & Management

S. V. Patil[1] and Dr. S. D. Khamitkar[2]

[1] SRTM University

Received: 15 December 2012 Accepted: 3 January 2013 Published: 15 January 2013

Abstract

Mobile agents have special characteristics which can help intrusion detection in several ways. The use of mobile codes and mobile agent based computing paradigms has been proposed in several researches till date. In this paper we try to present a scope for the possible association of Mobile Agents in the field of network security and management.

Index terms— mobile agent, network security, intrusion detection.

1 I. Introduction

obile Agents are composition of computer software and data which migrates from one computer to another. While doing this, they continue their itinerary up to the home computer. Autonomy and mobility are main features of mobile agents, specifically mobile agent is a process where mobile agent moves from one environment to another environment, with remains data intact. Mobile agent it self decides when and where to move. When a mobile agent decides to move then they save their own state and this state transport to another host. Mobile agents are specific about mobile code and they are choose the host and also active in respect of execution [1,4].

Mobile agents have special characteristics which can help intrusion detection in several ways. The use of mobile code and mobile agents computing paradigms have been proposed in several researches. The advantages include: overcoming network latency, reducing network load, executing asynchronously and autonomously, adapting dynamically, operating in heterogeneous environments, and having robust and fault-tolerant behavior. Moreover implementation of mobile agents in languages such as JAVA, provides mobile agents with system and platform independence and considerable security features [1,7].

As computer network is a collection of autonomous connected computers and other communication devices used for sharing resources or computers uses wired or wireless links as transmission media. Network security is an important task that must be seriously considered when designing a network. Network security is defined as the policies and procedures followed by a network administrator to protect the network devices from threats and simultaneously the unauthorized users must be prevented from accessing the network [2]. Maintaining Network security is a broad subject means securing our network from unauthorized entity or Mal ware. The unauthorized entity may modify the information or accessing the network through remote computer may harm the network. Following are some network security measures, 1. Availability : The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it.

2. Integrity : Integrity guarantees the identity of the messages when they are transmitted.

2 Confidentiality : Confidentiality means that certain

information is only accessible to those who have been authorized to access it. 4. Authenticity : Authenticity is essentially assurance that participants in communication are genuine and not impersonators. 5. Non repudiation : Non repudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message.

6. Authorization : Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority.

3 II. Literature Review and Findings

In this section we are reviewing some literature related with Mobile agent and Network management and security. Once the mobile agent has migrated, the connection between the client and server is disconnected, later when mobile agent finishes its job at the server, then it will reconnect to the client or host. This clearly saves the network bandwidth especially in the wireless environment where disconnection is frequent and bandwidth play a major role [3]. A Mobile agent (MA) is a composition of computer software and data which is able to migrate (move) from one computer to another autonomously and continue its execution on the destination computer. Taking the recent development i.e. going to this field, mobile agent based intrusion detection system is an efficient way to the intrusion detection in the distributed environment. [4] . Mobile agents perform a task by migrating and executing on(D D D D D D D D)

detection, the network administrator sends some special types of mobile agents in the network and collects information from different nodes. After analyzing this information the network administrator can identify the computer system running in promiscuous mode. [5] In [1] evaluate the implications of applying mobile agent technology to the field of intrusion detection and present a distributed intrusion detection system (IDS) based on mobile agents that considers large-scale network environment in order to monitor multiple hosts connected via a network as well as the network itself. Once system will be operational it will be the first comprehensive real-life application using mobile agents that will not only provide security to network resources but also provide security and protection to the mobile agents system itself. The system efficiently solves several problems with the existing IDS/IPS solutions: it can detect new vulnerabilities, it can process and filter large volumes of logs, it reacts to intrusions in realtime, provides protection against unknown attacks, supports and improves IDS/IPS commercial products by different vendors, and handles software patches. The system not only improves the existing IDS/IPS solutions, but it also eliminates several of their core problems. In addition, it is self protected by full encryption, both mobile agents and their platforms, and therefore not vulnerable to attacks against its own components and resources. [6]

4 III. Discussions on Network Security & Management using Mobile Agents

There exist many contemporary approaches for network security categorized as Host based and Network based. However, they work for Intrusion detection and not for overall security management. As mentioned earlier, Mobile Agents can be useful in such places where we need network security as well as network management. We can use different mobile agents for securing the network from the threats as well as detect the threats. For example, network sniffing detector mobile agent used to find the network sniffer program in the network. Mobile agents can be used in above context as follows: a) Network load Reducing : Due to the multiple interactions in network, it creates excess network traffic. A mobile agent through the package conversation they dispatches the packets on the destination host at that time locally interaction happens and it helps to reduce the network load. b) Overcome Network Latency : In real time systems, with the help of mobile agents overcome the network latency, because mobile agents dispatches from central controller and acts locally. c) Tolerant to Network Faults : Without active connection between clients and server mobile agents can operate. d) Encapsulate Protocols : When data is being exchanged in network at that time every host has a code, for this code needs protocols e.g. incoming and outgoing. When these protocols needs security at that time protocol code becomes heavy and creates problems. Mobile agents move on the remote host and using specific channels creates new protocols. e) Execute Asynchronously and Autonomously : It is possible to embedded different tasks in the mobile agents and may be dispatched on the hosts. When agents are dispatched they becomes independent from the process and due to this mobile agents become asynchronous and autonomous. f) Adapt Dynamically : Mobile agents have their own sense about execution environment, because they reacts autonomously with the changes. They solve specific problem in the network by their own. g) They are Naturally Heterogeneous : Network computing is itself heterogeneous in respect of hardware and software; therefore mobile agents are also heterogeneous in nature. [7] In case of network management, the Mobile agents assist to the network administrator to manage the network security. For security management mobile agent's team launched in the network this team visits to all the computers in the network and different services security software analyzes and install. For this mobile agents uses following techniques 1. Connectivity and states of remote hosts are checked and reported. 2. Configuration of remote hosts are cheeked and recorded. 3. Security configuration management related tasks are applied. 4. Mapping of snort rules and identified vulnerabilities.

For completing the above four function mobile agents team automating launched, these teams interact with the all system and install security tools on the remote hosts and complete the desired network security management tasks.

Similarly we can detect intrusions also. Intrusion detection is implemented by an intrusion detection system and today there are many commercial intrusion detection systems available. In 1987 Dorothy E. Denning proposed intrusion detection as is an approach to counter the computer and networking attacks and misuses. In general, most of these commercial implementations are relative ineffective and insufficient, which gives rise to the need for research on more dynamic intrusion detection systems [8].Mobile agents plays very important role in the network security. Mobile agent searches the malicious activity in the network, for these work mobile agents provides

following three groups. The capacity of these teams to analyses the logs, these logs created from sensors e.g. Snort, Osiris and MS Windows firewall which are present on the host computers. [6] Mobile agent reaches on the remote hosts, analyses the logs and if any serious problem then reports to the security administrator. At the same time second team of mobile agent reaches on the remote host and continuously snorts, monitor and analyze, if this team finds any suspicious activity calls the new mobile agents and lastly the third team of mobile agents detects intrusion activity.

Above case can be extended for Distributed systems also. Today, computer system has evolved into a distributed computing machine, nothing is static now, not even the security threats and attacks. The security issues are of high concern today. In the world of open environment problem faced widely by the computer system and network is the network intrusion. [4] Intrusion detection system is the security mechanism that gathers and analyses the information to detect unwanted attempts of accessing and manipulating the user and system activities and report it to the management section.

As an example, MAIDS was developed by Lowa State University is a distributed IDS based on mobile agent technology. It build a model for an intrusion activity with software fault tree analysis (SFTA), and transform the SFTA model into intrusion detection by the use of Colored Petri net (CPN). Intrusion detection in MADIS is not only relied on direct linked neighbors of a particular host but also other hosts in the network. In this way the original host can obtain more information to achieve a more accurate decision. Mobile agent may enhance the performance of IDS and even offer IDS some new capabilities, however these benefits is not easy obtained. We could learn from these existing system that there are three main research areas in IDS with mobile agent technologies, MAIDS can gather information not only from neighbors of the compromised hosts but from more other hosts in the network that can lead to more accurate final decision. [9] IV.

5 Conclusion

Mobile agent provides an interestingly new way of network security & management. However, the security, infrastructure and standardizing issues still represent significant constraints. The main thing from our findings is that mobile agent has the potential in increasing the performance of network management. Due to its nature of being an innovative way from the programming environment, but some work is still required. [1]

1

Figure 1: E 1 .

[1] Eseveral hosts connected to the network. For the sniffer

[Singh et al. (2012)] , Yashpal Singh , Kapil Gulati , S Niranjan . *DIMENSIONS AND ISSUES OF MOBILE AGENT TECHNOLOGY International Journal of Artificial Intelligence & Applications (IJAIA)* September 2012. 3 (5) .

[Shiv Shakti Srivastava et al.] 'A Survey on Mobile Agent based Intrusion Detection System'. Nitin Shiv Shakti Srivastava , Saugata Gupta , Saurabh Ghosh , Chaturvedi . *International Symposium on Devices MEMS, Intelligent Systems & Communication (ISDMISC) 2011, Proceedings published by International Journal of Computer Applications®*, IJCA.

[Mohammad Sazzadul Hoque et al. (2012)] 'AN IMPLEMENTATION OF INTRUSION DETECTION SYSTEM USING GENETIC ALGORITHM'. Md Mohammad Sazzadul Hoque , Md. Abu Naser Mukit , Bikas . *International Journal of Network Security & Its Applications (IJNSA)* March 2012. 4 (2) .

[Dr et al. ()] 'Distributed Intrusion Detection System using Mobile Agents'. Bhushan Dr , Jayant Trivedi , Chintan Rajput , Pinky Dwivedi , Jobanputra . *International Symposium on computing, Communication, and Control (ISCCC 2009) Proc .of CSIT*, 2009. 2011. 1.

[Muftic ()] 'INTRUSION DETECTION AND PREVENTION SYSTEM USING SECURE MOBILE AGENTS'. Muhammad Awais Shibli Sead Muftic . *IEEE INTERNATIONAL CONFERENCE ON SECURITY AND CRYPTOGR-APHY* JULY 2008. p. .

[Mishra (2012)] 'Mobile Agents: As a Solution for Sniffer Detection'. Amit Mishra . *International Journal of Computer Technology and Electronics Engineering (IJCTEE)* August 2012. 2 (4) .

[Mr et al. (2012)] 'Network Security Using IP firewalls'. Mr , Mr Sachin Taluja , Pradeep Kumar , Verma . *International Journal of Advanced Research in Computer Science and Software Engineering* August 2012. 2 (8) .

[Jain and Raghuwanshi ()] 'NEW MOBILE AGENT-BASED INTRUSION DETECTION SYSTEMS FOR DISTRIBUTED NETWORKS'. Pranita Jain , Sandeep Raghuwanshi , PateriaR . *International Journal of Wireless Communication* 2011. 1 (1) p. .

[Lange and Oshima (1999)] 'Seven Good Reason for Mobile Agents'. Danny B Lange , Mitsuru Oshima . *Communications of the ACM* March 1999. 42 (3) p. .