Agent Based Network Sniffer Detection

S. Dhanalakshmi and A.R.M. Ravi Shankar

Abstract *- Network sniffing was considered as a major threat to network and web application. Every device connected to the Ethernet-network receives all the data that is passed on the segment. By default the network card processes only data that is addressed to it. However listening programs turn network card in a mode of reception of all packets – called promiscuous mode. As we know sniffer is a program that eavesdrops all the data moving onto the network [1]. In this mode the NIC does not perform its basic task of filtering. The NIC forwards all the packets moving in the network to the system for further processing. Sniffer does not generate any traffic in the network, so it can not be detected easily. Many sniffers like wireshark, Cain & Abel, ethersniff etc. are available at no cost on the internet. There are many proposed solutions are available for the detection of network sniffing including antisniff [2], SnifferWall [3], Sniffer Detector [4] etc. but any solution does not guarantee full security. Here in this paper we are proposing Mobile Agents as a solution for the problem of sniffer detection. Mobile agents perform a task by migrating and executing on several hosts connected to the network. For the sniffer 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.*

Index Terms*—Computer Security, Mobile Agent, Sniffer, Sniffer Detection*

I. INTRODUCTION

COMPUTER networks including internet are continuously growing in both complexity and size. Computer networks are the backbone of an organization. So the computer security is now a main concern for any organization. Network threats can be classified in two categories:-

1. External Threats
2. Internal Threats

Some survey reports are showing a fact that more than 85 percent of network threats are generated by internal employees of a company. We can use different tools like Firewall for the protection against the external threats, but internal threat detection is not so easy. Sniffer comes in the category of internal threat. It is basically a program by which any person can see all the data and its movement in the Network. Here in this paper we are suggesting the Mobile Agents [2] as a tool for sniffer detection.

II. METHODOLOGY

A mobile agent consists of the program code and the program execution state (the current values of variables, next instruction to be executed, etc.) [5]. initially, a mobile agent resides on a computer called the home machine.

The agent is then dispatched to execute on a remote computer called a mobile agent host (a mobile agent host is also called mobile agent platform or mobile agent server). When a mobile agent is dispatched the entire code of the mobile agent and the execution state of the mobile agent is transferred to the host.

The host provides a suitable execution environment for the mobile agent to execute. The mobile agent uses resources (CPU, memory, etc.) of the host to perform its task. After completing its task on the host, the mobile agent migrates to another computer. Now in next section we present the overall system architecture for sniffer detection using mobile agents

III. LITERATURE SURVEY

As we know today information security is a main field for the research and many researchers have been contributed for the same. There are many solutions that have been proposed for the computer security.

A solution was proposed by Kshirsagar, D.D. in which they suggested intrusion detection system containing five modules named: Capture Module, Decode Module, Detection Module, Known Attack Pattern Module and Action Module [6].

This is an efficient technique but it is complex and it also depends on the known attacks. Similarly a solution proposed named Sniffer Wall [3] also exists. Here in this paper, advanced technology of Mobile Agent has been proposed as a solution of Sniffer Detection

IV. SYSTEM ARCHITECTURE

The architecture is made up of following components:

1. Network Administrator
2. Mobile Agent Platform
3. Mobile Agent for detection

We are considering the Network Administrator also as a component because he or she will generate the mobile agent, monitor them and analyze the information provided by the mobile agent for the security purpose.

Mobile Agent Platform is basically providing all the services like creation, interpretation, execution, transfer and termination for the mobile agents [7]. This platform is

S.Dhanalakshmi, Department of Computer Science and Engineering, Arunai Engineering College, Tiruvannamalai, India. E-mail:danalakshmi1984@gmail.com

A.R.M. Ravi Shankar,Department of Computer Science and Engineering, Arunai Engineering College, Tiruvannamalai, India. E-mail:muraliravishankar@gmail.com

© 2015 psnajournals

responsible for accepting instructions given by network administrator, sending mobile agents to other nodes etc.

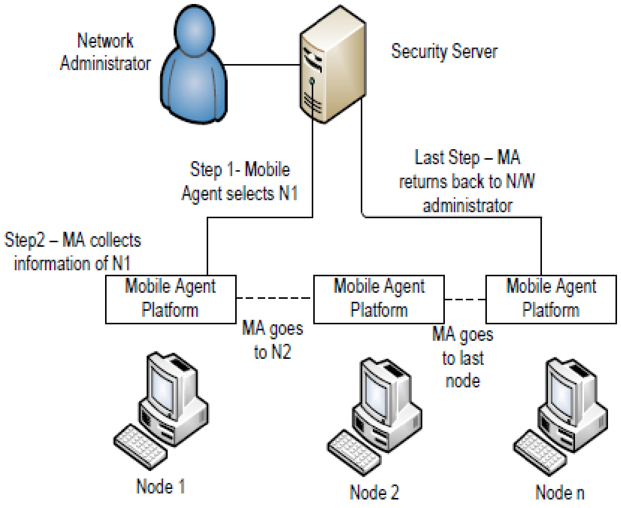

Figure 1: Experimental Setup

Mobile Agents are the main component of this architecture. They are specially designed to perform network analysis task. Whenever a mobile agent starts execution on a specified node, it monitors all the incoming and outgoing network traffic for that node. If it finds any abnormal incoming traffic (in the case of sniffer) or any other malicious activity, it immediately sends an alarm message to the network administrator for necessary action

V. DESIGN

The following algorithm can be used for the detection of sniffer in the network.

Algorithm

1. Network administrator installs and configures Mobile Agent Platform on all the computers connected in the Local Area Network (LAN)
2. Now whenever the whole system starts, the network administrator activates some specially designed mobile agents.
3. Now these mobile agents travel in the network and select any random node for execution.
4. Mobile Agent collects all the information about network activities including network traffic for that node.
5. As we know if any node runs a Sniffer, then it collects all the packets moving in the network. So mobile agent sends an alarm message to the network administrator if it finds that the incoming network traffic is greater than a pre specified value.
6. After receiving this alarm message, network administrator can take necessary action.
7. If everything is normal then the mobile agent moves to another node and repeats the steps 4 and step 5.

So this whole process can detect the sniffer present in the network. For the mobile agent implementation, we use aglets2.5-alpha which is a java based tool and freely available on the internet

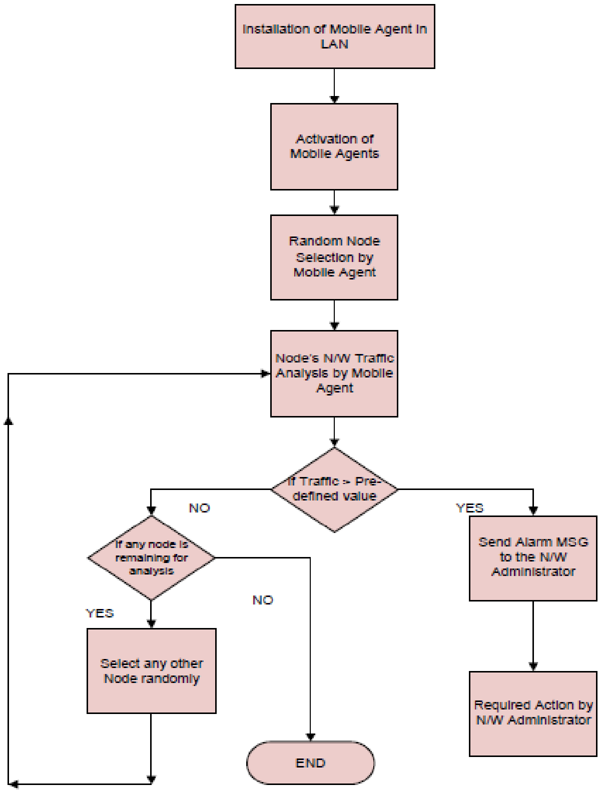
Installation of Mobile Agent In LAN
Activation of Mobile Agents
Random Node Selection by Mobile Agent
Node's N/W Traffic Analysis by Mobile Agent
If Traffic > Pre-defined value
NO
YES
If any node is remaining for analysis
Send Alarm MSG to the N/W Administrator
YES
NO
Select any other Node randomly
END
Required Action by N/W Administrator

Figure 2: Process of Sniffer Detection

So now using this algorithm we can detect sniffing activities in the network).

VI. CONCLUSION

The whole idea depends upon a real life situation in which a policeman visiting all the streets randomly and if he finds any thing unusual, he reports to the police station. Similarly our mobile agent selects any node randomly and investigates that node, if it finds excessive incoming traffic on the network interface card then report to network administrator. So the sniffer can be detected.

However if intruder makes some changes in our mobile agent platform or mobile agent, then it may fail the whole process. So in future, some more security measures should be taken for the guaranteed security.

REFERENCES

[1] Amit Mishra "Techniques to Abolish the Effect of Sniffer Existing in the Network" International Journal of Computer Information Systems Sep 2011

[2] Anti sniffing: http://www.securitysoftwaretech.com/antisniffing,

[3] H. M. Kortebi AbdelallahElhadj, H. M. Khelalfa, An experimental sniffer detector: Snifferwall, (2002).

[4] Thawatchai Chomsiri, Sniffng packets on LAN without arp spoofing, Third 2008 International Conference on Convergence and Hybrid Information Technology (2008).

[5] http://en.wikipedia.org/wiki/Mobile_ agent

© 2015 psnajournals

[6] D.D. Kshirsagar, "Network Intrusion Detection based on attack pattern" Vol 5 Pp. 283-286

[7] Parineeth M Reddy "Mobile Agents Intelligent Assistants on the Internet"

[8] M. Eid, "A New Mobile Agent-Based Intrusion detection System Using distributed Sensors", in proceeding of FEASC, 2004.

© 2015 psnajournals