Agent Based Network Sniffer Detection

A.R.M. Ravi Shankar*, K. Mahesh**

* Department of Computer Science & Engineering, Arunai Engineering College
** Department of Computer Science & Engineering, Arunai Engineering College

Abstract- A Sniffer is a program on the network traffic by grabbing information travelling over a network [1]. Many people assume computers connected to a switch are safe from sniffing here we go for Antisniffing [2]. Nothing could be further from the truth. Computers connected to switches are just from vulnerable to sniffing. Computers connected to switches are just as vulnerable to sniffing as those connected to a hub. Here in this paper we propose Mobile Agents to detect sniffers. Mobile agents perform a task by migrating and executing on several nodes connected to the network. Ignored to detect sniffers [3], 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

Packet sniffing is a technique of monitoring every packet that crosses the network. In theory, it's impossible to detect these sniffing tools because they are passive in nature, meaning that they only collect data. While they can be fully passive, some aren't therefore they can be detected. This paper discusses the different packet sniffing methods and explains how AntiSniff tries to detect these sniffing programs.

II. METHODOLOGY

A mobile agent[5] is a software agent that has the additional property that it is not bound to operate only in the system in which it started. A mobile agent is autonomous because it may decide itself where it will go, what it will do there, and how long it will exist for. However, its environment or other mobile agents may also influence it.

Although mobile agents do not provide a solution to any previously unsolvable problems, they do have advantages over other technologies. They can be used to benefit or to simplify different types of application areas. Some examples of these application areas include ecommerce, distributed information retrieval, telecommunication networks services, and monitoring and notification.

Adaptive Learning: Mobile agents[6] can learn from experiences and adapt themselves to the environment. They can monitor traffic in large networks and learn about the trouble spots in the network. Based on the experiences of the agent in the network the agent can choose better routes to reach the next host.

Autonomy: Mobile agents can take some decisions on its own. For example, mobile agents are free to choose the next host and when to migrate to the next host. These decisions are transparent to the user and the decisions are taken in the interest of the user.

Mobility: Mobile agents have the ability to move from one host to another in the network.

III. LITERATURE SURVEY

Packet Sniffing Tools: developers debugging communication protocol implementations, or anyone trying to learn how their networks work. Because attackers use sniffers for network reconnaissance and to intercept transmitted credentials and data, learning about the capabilities and limitations of packet sniffers is an important facet of understanding the security risks.

Tcpdump is the most widely used UNIX/Linux tool to record network traffic. It captures packets based on a wide range user-specified criteria, and can save the traffic in different formats. Tcpdump is commonly included in most Linux distributions.

Wireshark is the most widely used graphical application for network monitoring and analysis. It is open-source and runs on most popular computing platforms, including UNIX, Linux, and Windows..

IV. SYSTEM ARCHITECTURE

Here The architecture consists of the following components:

- An intrusion detection processor,
- Network Administrator,
- Mobile Agent Platform,
- Mobile Agent for detection.

Mobile Agent Platform is basically providing all the services like creation, interpretation, execution, transfer and termination for the mobile agents. This platform is responsible for accepting instructions given by network administrator, sending mobile agents to other nodes etc.

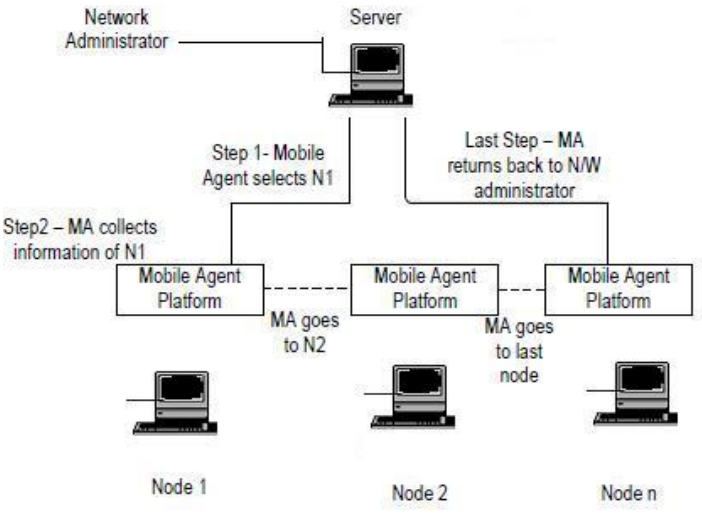

Fig.1 Architectural View

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 steps can be used for the detection of sniffer 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. This part we present the architecture of our distributed IDS.
The architecture consists of the following components: (1) an intrusion detection processor, (2) a mobile agent platform, and (3) network administrator, (4) mobile agent for detection.

A. Data Flow Capture

As the main network node monitor, the Data Flow Capture network traffic which incoming monitors, it captures dump of data and sends to IDA for detecting intrusion, then, Data Analysis component to analyze and self-learning.

B. Intrusion Detection Agent (IDA)

IDA is the most important component of the system. It is responsible for monitoring network segments (subnets), and acts as a central intrusion detection agent and data processing unit. The unit is placed on a node that entry into intranet to monitor network traffic for all devices on the segment. And it is setup to send alert in time, so that, checking the errant packets using rule sets when it enter into the segment. Its main capabilities is detecting intrusion and judging whether the behaviour is abnormal, if it is abnormal, alerting to Administrator or make some decisions.

C. Sniffer Detection Techniques

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

VI. CONCLUSION

Distributed computing involving several computers in a network can be achieved using message passing or remote procedure calls (RPC). The recently developed mobile agent technology adds a new dimension to distributed computing. Experts suggest that mobile agents will be used in many Internet applications in the years to come.

However there still exist many technical hurdles that need to be tackled, the most important of them being security. Only when security issues are properly addressed, will the mobile agent technology be widely accepted. 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. 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.

REFERENCES

[1] Sumit dhar “Sniffer intrusions” – network security.
[2] Antisniffing: 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 spooffing, Third 2008 International Conference on Convergence and Hybrid Information Technology (2008).
[5] http://en.wikipedia.org/wiki/Mobile_ agent
[6] Network Management with mobile agents"-Andrzej Bieszczad

AUTHORS

First Author – A.R.M Ravi Shankar, M.C.A., M.E., Arunai Engineering College, muraliravishankar@gmail.com.
Second Author –K. Mahesh. M.E., Arunai Engineering College, mbmaheshbabu5@gmail.com.