ISSN No. 0976-5697

Volume 2, No. 4, July-August 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Mobile Agent Based Suspicious Packet Detection Technology

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

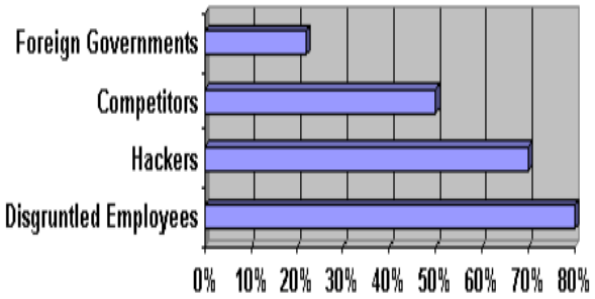
Dr Nidhi Taneja
Department of Electronics & Comm. Engineering,
Delhi Technical University, India
nidhi.iitr@gmail.com

Abstract: This paper presents an intrusion detection system (IDS) based on mobile agents that detect intrusion from outside the network segment as well as from inside. As network attacks have increased in number and severity over the past few years, intrusion detection systems have become a necessary addition to the security infrastructure of most organizations. This research paper presents the intrusion detection, developed for those who need to understand what security goals intrusion detection mechanisms serve, how to select intrusion detection systems for their specific system and network environments, how to manage the intrusion detection systems, and how to integrate intrusion detection functions with the rest of the organizational security infrastructure.

Keywords: Communication technology, IDS, mobile agent, MAP, network security.

I. INTRODUCTION

A. "Why Malicious Packet Detection?"



Attacks come from both the inside and the outside. As the survey in the following chart illustrates, disgruntled employees actually represent a larger threat and typically cause more damage than hacker attacks. An effective Intrusion Detection solution should detect attacks from both inside and outside the network.

B. Mobile Agent Technology

A mobile agent system is a combination of a client and a server which, when located on host computer runs, sends and receives mobile agents, and attempts to guard against mobile agents which attempt misuse. It provides or interfaces with the environment in which the mobile agent runs. In the terms of agent, there are two different of views from end-user perspective and from system perspective. From end-user perspective, an agent is only a program that can assists people and acts on the behalf and from the system perspective, agent is a software object that is situated within an execution environment, possesses the following mandatory properties

a. Reactive: could sense changes in the environment and acts according to those changes.
b. Autonomous: had control over its own actions.
c. Goal-driven, temporally continuous: (continuously executing) and may possess any of the following orthogonal properties – communication (able to communicate with other agents)
d. Mobile: can travel from one host to another.
e. Learning: adapt in accordance with previous experience.
f. Believable: appears believable to the end user.

Mobile Agent is not bound to the system where is begins execution, it could transport itself from one system in a network to another; with this ability, the agent can move to a system that contains an object with which the agent wants to interact and then to take advantage of being in the same host or network as the object [1]. If we apply MA as the tool to perform IDS or even better, make MA part of IDS, it means maximizing the potential of MA in the environment of IDS. Such can include

a. Platform independent IDS (it can then scan computers of different operating system in a network).
b. MA can also directly retrieve data from the network, scan and only bring back the results to the host (this will definitely reduce network load).
c. MA can perform port scanning and other IDS feature autonomously
d. Several MA can be deployed to different host of a single network, thus speeding up work. The results can be later compared when MAs exchange results among themselves.
e. Isolating the source and target. When automatic response may fail at the target and source, the final response is needed to limit an attacker's actions. Mobile agents can travel around all the computer components to perform remedial specified measure.
f. Mobile agents can run in heterogeneous environments and have high survivability.

Mobility is not required for software to be considered an agent. Agents are mobile when designed to be transported from one device to another. They are similar to programs submitted via Remote Job Entity, or macros embedded in e-mailed documents. Contrary to popular belief, mobile agents do not transport themselves, but depend on mobile agent systems to move their binary images over a variety of media To be effective, mobile agent systems must be deployed on all the devices to which a mobile agent may travel. Mobile agent systems may

implement special network protocols, header formats, and security techniques.

II. MOBILE AGENTS APPLICATION IN INTRUSION DETECTION

A. IDS Requirements

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

a. Functional Requirements:

i. The IDS must continuously monitor and report intrusion
ii. The IDS should have a very low false alarm rate
iii. The IDS must provide enough information to repair the system in the case of intrusion detection
iv. 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.
v. The IDS should be adaptive to network topology and configuration changes.

b. Performance Requirements:

i. Intrusion should be detected in real-time and reported immediately to minimize the damage to the network,
ii. The IDS must be scalable to be able to handle the additional computational and communication load.

c. 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.

i. 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.

ii. 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.

iii. 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[2].

iv. Adapting Dynamically

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

v. 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. In other words, as long as the installation of mobile agent platform, mobile agent can run on any network node in theory.

vi. 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.

d. IDS Limitations

The most common IDS shortcomings include the following:

1. Higher number of false positive,
2. 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 .
3. 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.

e. 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.

i. 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

III. STRENGTHS OF INTRUSION DETECTION SYSTEMS

A. Intrusion Detection Systems Perform The Following Functions Well

a. Monitoring and analysis of system events and user behaviors

b. Testing the security states of system configurations.
c. Base lining the security state of a system, then tracking any changes to that baseline
d. Recognizing patterns of system events that correspond to known attacks
e. Recognizing patterns of activity that statistically vary from normal activity
f. Managing operating system audit and logging mechanisms and the data they generate
g. Alerting appropriate staff by appropriate means when attacks are detected.
h. Measuring enforcement of security policies encoded in the analysis engine
i. Providing default information security policies
j. Allowing non-security experts to perform important security monitoring functions.

B. Two Primary Types of HIDS Can be Distinguished

a. Systems that monitor incoming connection attempts (Real Secure Agent, Port Sentry). These examine host-based incoming and outgoing network connections. These are particularly related to the unauthorized connection attempts to TCP or UDP ports and can also detect incoming ports cans.
b. Systems that examine network traffic (packets) that attempts to access the host. These systems protect the host by intercepting suspicious packets and looking for aberrant payloads (packet inspection).
c. Systems that monitor login activity onto the networking layer of their protected host. Their role is to monitor log-in and log-out attempts, looking for unusual activity on a system occurring at unexpected times, particular network locations or detecting multiple login attempts
d. Systems that monitor actions of a super-user (root) who has the highest privileges (Log Check). IDS scans for unusual activity, increased super-user activity or actions performed at particular times, etc.
e. Systems that monitor file system integrity (Tripwire, AIDE). Tools that have this ability (integrity checker) allow the detection of any changes to the files that are critical for the operating system [3].
f. Systems that monitor the system register state (Windows platform only). They are designed to detect any illegal changes in the system register and alert the system administrator to this fact.

IV. INTRUSION DETECTION SYSTEM

Most traditional intrusion detection systems take either a network-or a host-based approach to recognizing and deflecting attacks. When an IDS looks for these patterns in network traffic, it is network-based. When an IDS looks for attack signatures in log files, it is host based. Each approach has its strengths and a weakness each is complementary to the other. An efficient IDS will adopt both technologies. The definition of intrusion detection system does not include preventing the intrusion from occurring, only detecting it and reporting it to an operator. The diagram in figure 1 below shows the classification of current IDSs.

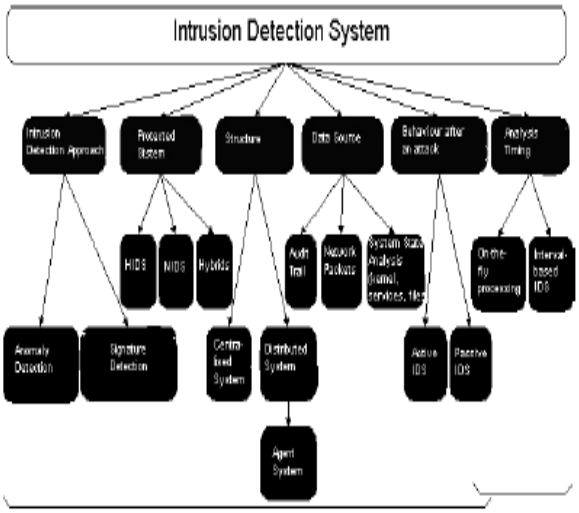


Figure 1.Classification of IDS

A. Implementation Phase Consists Of Two Distinct Components

i. MA server application (MASA), which is seated in the server.
ii. MA client application(s) seated in all remote hosts

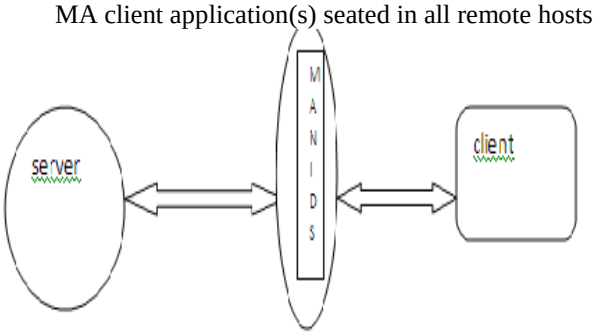


Figure 2. IDS with MA

a. Server Side

This component is the main intrusion detection processor. It is responsible for monitoring all remote hosts and acts as central processing unit. The main aim of the MASA is to launch the remote messaging mechanism to start the scanning of packets in the respective remote host. Its main capabilities are processing multiple logs sent by mobile agents, providing and updating rule and signature sets for each agent and interfacing the intrusion detection system to the system administrator.

b. Client Side

The remote mobile agent will travel to the remote host, together with appropriate information by the server. This agent is responsible for detecting intrusions based on data collected by sniffing and tracing the network traffic.
When the remote MA reached the target destination, it will trigger IDS in the remote host. The remote MA can also perform other instruction as instructed by the server MA. The remote host will then create another child to feedback to the MA server of event that has taken place in the remote host.

B. Audit Trail Processing

There are many issues related to audit trail (event log) processing. From the functionality point of view, recording every event possible means a noticeable consumption of

system resources (both the local system and network involved). Log compression, instead, would increase the system load. Specifying which events are to be audited is difficult because certain types of attacks may pass undetected. The main reasons for having an audit function include:

a. Detection of attack manifestations for post-mortem analysis.
b. Detection of recurring intrusion activity (yielding unauthorized privileges, abuse, attack attempts).
c. Identification of successful intruders.
d. Identification of own system weaknesses.
e. Development of access and user signatures and definition of network traffic rules that are important for anomaly detection-based Intrusion Detection Systems.
f. Repelling potential intruders by simply making them aware of the existence of the auditing means.
g. The audit reporting may provide a form of defense for an innocent user, for example possible involved in hacking attempts.
h. The log event-based IDS method needs to have the following capabilities.
i. Allowing of parameterization for easy recording of system event logs and user activities,
j. Providing an option of self-disengagement of logging mechanisms in the event of insufficient space or DoS attacks.
k. Audit trail processing using additional mechanisms because of large file sizes.
l. A reasonable minimum system resource consumption for auditing purposes.[4]

V. METHODOLOGIES OF NETWORK INTRUSION DETECTION

A. Anomaly vs. Signature Detection

Intrusion detection systems must be capable of distinguishing between normal and abnormal user activities, to discover malicious attempts in time. However translating user behaviors (or a complete user-system session) in a consistent security-related decision is often not that simple

- many behavior patterns are unpredictable and unclear In order to classify actions, intrusion detection systems take advantage of the *anomaly detection* approach, sometimes referred to as *behavior based* or attack signatures i.e. a descriptive material on known abnormal behavior (*signature detection)* also called *knowledge based.*

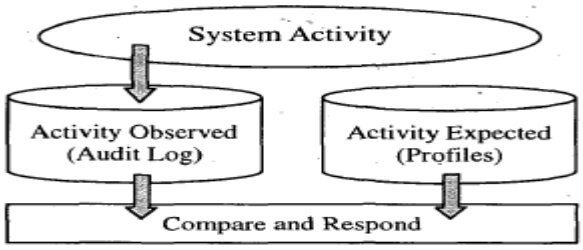


Figure 3 Anomaly detection

a. Normal Behavior patterns — Anomaly Detection

Normal behavior patterns are useful in predicting both user and system behavior [5]. Here, anomaly detectors construct profiles that represent normal usage and then use current behavior data to detect a possible mismatch between profiles and recognize possible attack attempts.

In order to match event profiles, the system is required to produce initial user profiles to train the system with regard to legitimate user behaviors.

b. Advantages of this Anomaly Detection Method are:

Possibility of detection of novel attacks as intrusions; anomalies are recognized without getting inside their causes and characteristics; less dependence of IDSs on operating environment (as compared with attack signature-based systems); ability to detect abuse of user privileges [6].

c. The biggest Disadvantages Of This Method are:

i. A substantial false alarm rate. System usage is not monitored during the profile construction and training phases. Hence, all user activities skipped during these phases will be illegitimate.
ii. User behaviors can vary with time, thereby requiring a constant update of the normal behavior profile database (this may imply the need to close the system from time to time and may also be associated with greater false alarm rates).
iii. The necessity of training the system for changing behavior makes a system immune to anomalies detected during the training phase (false negative)[7].

B. Misbehavior Signatures

a. Signature Detection

Systems possessing information on abnormal, unsafe behavior (attack signature-based systems) are often used in real-time intrusion detection systems (because of their low computational complexity).The misbehavior signatures fall into two categories:

i. Attack signatures – they describe action patterns that may pose a security threat. Typically, they are presented as a time-dependent relationship between series of activities that may be interlaced with neutral ones.
ii. Selected text strings – signatures to match text strings which look for suspicious action (for example – calling /etc/passwd).

Any action that is not clearly considered prohibited is allowed. Hence, their accuracy is very high (low number of false alarms). Typically, they do not achieve completeness and are not immune to novel attacks.

b. Advantages:

Very low false alarm rate, simple algorithms, easy creation of attack signature databases, easy implementation and typically minimal system resource usage.

c. Disadvantages:

i. They are inherently unable to detect unknown, novel attacks. A continuous update of the attack signature database for correlation is a must.
ii. Maintenance of an IDS is necessarily connected with analyzing and patching of security holes, which is a time-consuming process.
iii. The attack knowledge is operating environment–dependent, so misbehavior signature-based intrusion detection systems must be configured in strict compliance with the operating system [8].

C. There are Several Compelling Reasons to Acquire and use IDS (Suspicious Packet Detection)s:

a. To prevent problem behaviors by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the system.
b. To detect attacks and other security violations that is not prevented by other security measures.
c. To detect and deal with the preambles to attacks.
d. To document the existing threat to an organization
e. To act as quality control for security design and administration, especially of large and complex enterprises.
f. To provide useful information about intrusions that do take place, allowing improved diagnosis, recovery, and correction of causative factors.
g. Detecting problems that are not prevented by other security measures.
h. Detecting the preambles to attacks (experienced as network probes & other for existing vulnerabilities).
i. Documenting the existing threat.

VI. CONCLUSION

This paper present a modular prototype model for intrusion detection system based on mobile agent technology. In this paper, we proposed a novel classification of a typical intrusion detection system. This paper present an architecture and model of a scenario of an intrusion detection system based on mobile agents. This architecture aims to minimize the costs of IDS & ability to detect malicious activity is achieved by mobile agents to remote hosts to generate complete and meaningful tracing and detecting incoming packets using intrusion detection system. The future work will focus on the performance aspects and security issues of the system which have not been explored yet.

VII. REFERENCES

[1] Jai Sundar Balasubramaniyan, Jose Omar Garcia-Fernandez,David Isacoff, Eugene Spafford, Diego Zambon, “An Architecture for Intrusion Detection using Autonomous Agents”, COAST Laborator Purdue University West Lafayette 2003

[2] http://www.windowsecurity.com

[3] H.Safuan, Z.B.Cheah, H.W.Lim, J.H.Chin, “Intrusion Detection System Based on Mobile Agent”, Faculty of Information Science & Technology, Multimedia University Malaysia 2005.

[4] Dipankar Dasgupta and Hal Brian, “Mobile Security Agents for Network Traffic Analysis”, Intelligent Security Systems Research Group, Division of Computer Science,The University of Memphis 2005.

[5] Rebecca Bace1 and Peter Mell2, “Intrusion Detection System”, National Institute of Standards and Technology, Scotts Valley, CA 2005.

[6] M.Slagell,The design and Implementation of MAIDS (Mobile Agents for IntrusionDetection System), Master’s thesis, Iowa State University, May 2001.

[7] Gao Kun and 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. 2009

[8] Mojtaba Karami , Marjan Kuchaki Rafsanjani , Amir Hosein Fathi Navid and Yaeghoob Yavari, “Quantitative and Agent based Intrusion Detection System”, Department of Electrical and Computer Engineering, Department of Electrical and Computer Engineering, Islamic Azad University Hamedan Branch, Hamedan, Iran 2011.

