Enhanced Architecture for Misconfiguration and Intrusion Detection using Centralized Rule based System

Sanjeev Sharma, PhD.
School of information technology
R.G.T.U, Bhopal, India

Rajendra Kumar Tiwari
Computer Scie. & Engg.Department
B.I.S.T, Bhopal, India

Rahul Kumar Gour
Computer Scie. & Engg.Department
B.I.S.T, Bhopal, India

ABSTRACT
Web servers and web-based applications are popular attack targets. Web servers are usually accessible through corporate firewalls. The number of reported web application vulnerabilities is increasing dramatically. Thus the task of securing web applications is one of the most urgent. On the other hand traditional protection mechanisms like firewalls were not designed to protect web applications and thus do not provide adequate defense. Current attacks cannot be thwarted by just blocking ports 80 (HTTP) and 443 (HTTPS).Previously known intrusion detection systems are not efficient with more false positive alarms and more time and space complexity. In this research work a new IDS architecture is introduced which detect misconfiguration and intrusion simultaneously. There is also used a RBs (Rule Based System) which take appropriate action accordingly degree of misconfiguration. The RBs consist with predefined rule. This rules guide the system to take appropriate action. Rules are triggered as soon as it received signal for misconfigurations. The architecture designed such a way that it can handle misconfigurations and detection of intrusion simultaneously.

KEYWORDS
Intrusion Detection, Mobile Agent, Network Security.

1. INTRODUCTION
Now a day's network application can be found anywhere so that the security of network becomes critical Because of the wide spread of cracking, technology, and new attack methods come forth quickly and become more and more complex. Static firewall is not enough to solve all kind of attacks, so the intrusion detection system (IDS) should be adopted. Computer networks connected to Internet are always exposed to many kinds of cybercrimes [15]. An Internet user with malicious intent can access, modify, or delete sensitive information present on other computers or make some of the computer services unavailable to other users [13]. The infrastructure of current computer networks is so huge and complex that it is almost impossible to completely secure such networks. Various type of IDS system has been proposed. Most of them are based on the concept of identify the presence of intruder in log files. For analyze intruder IDS check the behavior of user, study the knowledge base details, & monitor the traffic on the network of log file. In this paper present an approach to check the misconfiguration on the log file. A rule based system is introduced to take action against misconfiguration.IDS with web log files are very flexible, efficient and scalable because Log file are simple plain text file which record information about each user access. It contains information about user ID, IP address, date, time, bytes transferred, access request. In this research work proposed architecture for checks the configuration of the log file on rule based system and then identifies the intrusion detection on that log file.

2. INTRUSION DETECTION SYSTEM
IDS is a set of software and hardware resource that can find activities endangering information security proactively in good time[11].IDSs are considered as a powerful detection tool to secure the computer network environments. These systems collect activities from the protected network and analyze them to generate alerts if the IDS detect an intrusion. The activities will be usually collected from the network packets stream and the host log file[12].an intrusion detection system (IDS) is needed to detect and respond effectively whenever the confidentiality, integrity, and availability of computer resources are under attack [14].Intrusion Detection Systems (IDS) is defined as a component that analyses system and user operations in computer and network systems in search of activities considered undesirable from security perspectives [3].Intrusion means to interrupt someone without permission. Intrusion is an attempted act of using computer system resources without privileges, causing incidental damage. Intrusion Detection means any mechanism which detects the intrusive behavior. Intrusion Detection System (IDS) monitors network traffic and its suspicious behavior against security. If it detects any threat then alerts the system or network administrator. The objective of IDS is to detect and inform about intrusions [2].IDS monitor the activity of the network with the purpose of identifying intrusive events and can take actions to abort these risky events [8].

3. RELETED WORK
Since last one decade network based intrusion detection is hot and burning issues. There are various technique introduced.

3.1 Distributed Intrusion Detection System using Mobile Agents
This work 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. The design and implementation part of author relies on Security Agents which monitor network traffic and report intrusion alerts to a central management node. This paper model comprises four major components: the IDS monitor, the Agent server which distributes intelligent mobile agents called mobile IDS agents, Authentication and Utility tool. This work not covers mobile agent's intercommunication and negotiation which can help

investigative mobile agents to share their knowledge. In addition intrusion pattern's knowledge sharing between IDS control centers can be considered for further studies [9][10].

3.2 Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents

In this work author emphasis on Signature based detection. Signature based detection is the most extensively used threat detection technique for Intrusion Detection Systems (IDS). One of the foremost challenges for signature based IDS systems is how to keep up with large volume of incoming traffic when each packet needs to be compared with every signature in the database. When an IDS cannot keep up with the traffic flood, all it can do is to drop packets, therefore, may miss potential attacks. Author proposes a new model called Dynamic Multi-Layer Signature based IDS using Mobile Agents, which can detect imminent threats with very high success rate by dynamically and automatically creating and using small and efficient multiple databases, and at the same time, provide mechanism to update these small signature databases at regular intervals using Mobile Agents [4].

3.3 LAMAIDS: A Lightweight Adaptive Mobile Agent-based Intrusion Detection System

This work presents a lightweight and adaptive mobile agent based intrusion detection system (LAMAIDS) that detects intrusion from outside the network as well as from inside. A main machine, being a typical intrusion detection system residing at a secure location, creates mobile IDS agents and dispatches them into the network. The mobile IDS agents are equipped with lightweight IDS capabilities and decision-making. On each hop, the agents sniff the network traffic and look for abnormal activities using a set of rules supplied by the main machine. Simulation results based on real-world scenarios demonstrate significant improvements in terms of detection rate, network overhead, and adaptability, scalability, and fault tolerance. This work treats three main challenges that face IDS, namely the ability to monitor local traffic and detect local intrusions, the dynamic evolvement of the detection rule-sets, and the immunity of the intrusion detection system itself [11].

3.4 New Mobile Agent-Based Intrusion Detection Systems for Distributed Networks

This work presents various distributed intrusion detection system (IDS), based on mobile agents, that detects intrusion from outside the network segment as well as from inside. The proposed model comprises three major components: The Network Intrusion Detection Component, the Mobile Agent Platform, and distributed sensors residing on every device in the network segment [9].

3.5 Misconfigurations Discovery between Distributed Security Components Using the Mobile Agent Approach

In this work authors emphasis on different network security component, such as firewall and intrusion detection system (IDS).For a perfect interoperability between these components in the network, these latter must be configured properly to avoid misconfiguration anomalies between them, However there are a set of anomalies between alerting rules in the IDS and filtering rules in firewalls, that degrade the network security policy. In this work, author's present a mobile agent based architecture to detect misconfigurations between these distributed components and generate a new set of rules free of errors [7].

3.6 Preprocessing of web server log file

The World Wide Web is a system of hypertext documents accessed via the Internet. World Wide Web gives large information to internet user. It is a huge repository of web pages and links. Web pages may contain text, images, videos, and other multimedia and navigate between them via hyperlinks. When user accesses websites are recorded in web logs file. Web server log file is a simple plain text file. Display of log file data in different format like W3C Extended log file format, NCSA common log file format, IIS log file format Log file contain noisy & ambiguous data which may affect result of mining process. To improve quality of data, log file should be preprocessed. One technique to detection of web attack is to analyze web server log file. This web attack means intrusion, Intrusion detection consists of procedures and systems created and operated to detect system intrusions [1].

4. PROPOSED WORK

In this research work, new mobile agent based architecture is proposed for multiple purpose. The aim of work is to detect misconfiguration and intrusion on the host/networks simultaneously. It is designed in such a way that it detects intrusion and takes appropriate action on intrusion/ misconfiguration in efficient way. Proposed architecture is based on the mobile agent so it is best solution in distributed environment. It detects misconfiguration and intrusion through web log file analysis. Basically working of proposed architecture is divided in two major phases.

Phase I: Misconfiguration management

Phase II: Intrusion detection

4.1 Misconfiguration Management

Misconfiguration can be occurring in many ways. For example, an application may unilaterally make seemingly innocuous changes to shared system configurations and cause unexpected behaviors in another application. A software bug may corrupt a Registry entry (by leaving a data field empty, for example).To diagnoses misconfiguration there is separate Mechanism is needed. In this research work a device which takes care about misconfiguration and take action accordingly called "controlling device". It accesses the log file of the clients. In this paper controlling device is a machine it's having rule based system which guide the system to take action according degree of misconfiguration. These research works identify misconfiguration through web log file analysis. Mobile agent traverses each node in the network periodically. It performs basically two major tasks. if mobile agent find no configuration then nothing to need take any action and move to next node otherwise(if misconfiguration detected) then it immediately send back details to controlling device (CD).

4.1.1 Rule Based System

Rule-based system is the domain-specific expert system that uses rules to make decision. Rule-Based Systems rely on sets of predefined rules each rule is mapped to a specific operation in the system. The rules serve as operational preconditions. If any log file is not configured properly so basis on the operation define on the RBs some action will be taken by the RBs. This action is:-

- Temporary block to the system.

- Send message to another device that this system is not properly configured.
- Correction on that misconfigured file.

4.1.2 Architecture for Check log file configuration

Mobile agent continuously traverses over the network and analysis configuration of log file. It conveys the response to controlling device about misconfiguration in log file. See Figure 1 depicts the overall working of it.

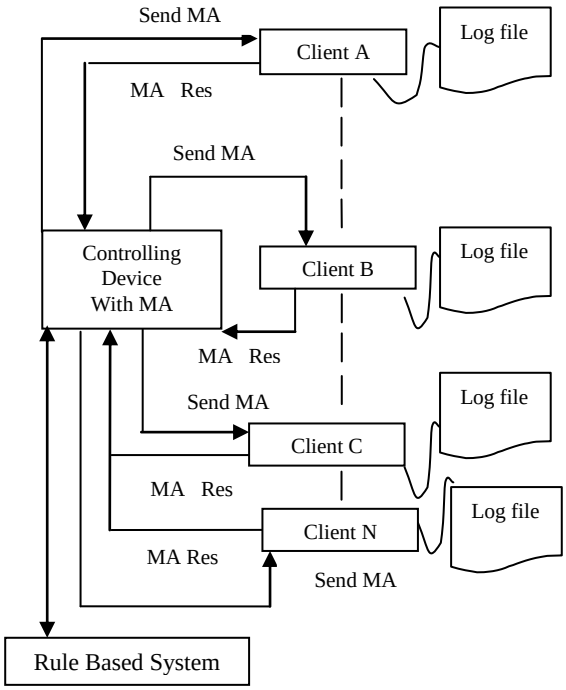

Figure 1: Architecture for log file configuration analysis

4.1.3 Algorithm for Misconfiguration

```
Input LFi  // Log Files
n= number of client / host in the network
Output:  MISCFD
RBs system: rule base system
Initialization:
i=1;
MAi = mobile agent
MISCFD
while ( i ≠ n) // traverse the network
{
        MISCFD= read (LFi)
        if (MISCFD ≠ ϕ)
                {
                Return MISCFD to RBs at CD
                }
        Move to next node
        i++
}
```

Figure 2: Algorithm for misconfiguration

MISCFD: MISCFD is stand for Misconfigured log data. This is a simple text file. That text file contain detailed of misconfiguration. If misconfiguration text file is empty, it means that log file is proper configured so move to next node. else it implies that there is some configuration problem with that node. Send MISCFD to controlling device which has rule base system. Controlling device take action accordingly degree of misconfiguration.

4.2 INTRUSION DETECTION

An intrusion is any unwanted activity either in the form of passive attacks or active attacks, which are used by the attackers to create undesired situation and harmful consequences for the user's confidentiality, network integrity or network resources availability. In simple words, any set of actions that try to compromise the data integrity, user's confidentiality or service availability can be termed as intrusion, while a system that attempts to detect such malicious actions of network or compromised nodes is called IDS. In this part we present a proposed architecture for intrusion detection, algorithm for applying mobile agent intelligence (MAI) and steps for identify intrusion.

4.2.1 Proposed Architecture for intrusion detection

The presented intrusion detection system Architecture is designed by applies MAI (Mobile agent intelligence) on the log file. Figure 3 depicts the overall working of it.

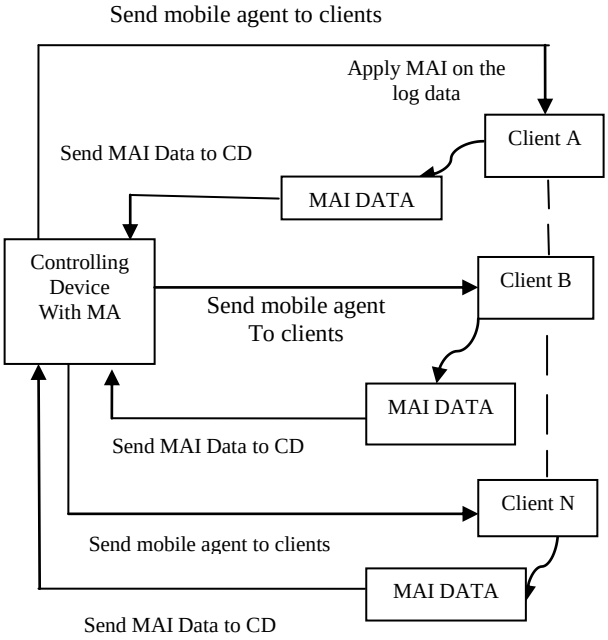

Figure 3: Architecture for intrusion detection

4.2.3 Algorithm for applying MAI on the log file

Mobile agent is designed for remote access or computation of data it reduces network traffic through performs data computation at remote/client side [5]. This characteristic make mobile agent best suitable in IDS system. Working of mobile agent is much like Remote procedure call (RPC), Remote method invocation [RMI] and .NET Remoting [6].

In this research work when mobile agent reaches at the client it applies its intellegence on the log file (log file is a simple plain text file which record information about each user) and send this MAI data to controlling device. Figure 4 represent the algorithm for applying MAI on log file.

In this algorithm the word $LFMAI_i$ means when mobile agent intelligence is apply on the LFi. Mobile agent extracts some component from the LFi and converts it into $LFMAI_i$

Input LF_i
n= number of client / host in the network
Output: APPNDLG
Initialization:
i=1;
MA_i = start mobile agent on the host
$EXTLOGF_i$
$LFMAI_i$
while (i ≠ n) // traverse the network
{
read (LF_i)
if ($LF_i \neq \Phi$)
{
Call MAI // apply mobile agent intelligence on the log file
MAI convert LF_i in to $LFMAI_i$ // extract important data
return $LFMAI_i$ to the controlling device
}
Move to next node
i++;
}

Figure 4: Algorithm for applying MAI on log file

When the intrusion detection is find on the controlling device. It takes some action against intrusion detection or keeps data for future analysis.

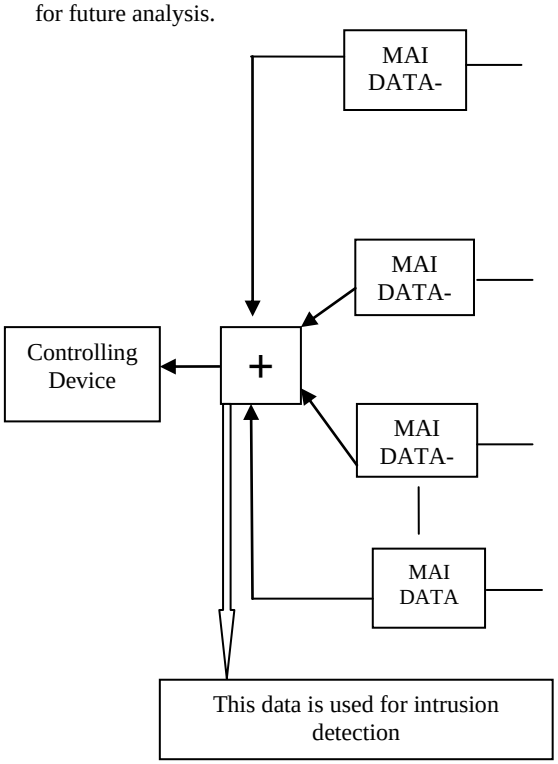

Figure 5: Work of Controlling Device

Figure 5 depicts that the entire mobile agent sends MAI data to controlling device. On the CD all data combined together and save it in controlling device memory for intrusion detection and pattern analysis of the user.

4.2.4 Steps for identifying intrusion

In this part we present steps to detect intrusion detection

- Initialization of controlling mobile agent
- Send controlling mobile agent to the client machine
- Apply MAI on the log file for extract data
- Collect MAI data from log file and copy it into new text file
- Transfer New log file to the controlling device
- Appending all new log file data into the controlling device log file
- Find intrusion detection on the appending log file data
- If intrusion find then
- Send message to appropriate system for taking some action
- Temporary blocked to related system
- End if
- Send positive response to the system

Figure 6: Steps for Intrusion detection

5. IMPLEMENTATION AND EXPERIMENTATIONS

For the implementation purpose a system Prototype has been developed by using remote method invocation in java Net Beans 7.2 IDE. Propose architecture is included in the implementation. The prototype consists of a user interface, clients and controlling device. The controlling device creates the mobile agent and the agent starts its journey it moves to the clients. During the journey, the agent visits some clients and performs its operation based up on rule base system. LAN, TCP/IP protocol and Windows XP are used as infrastructure of our prototype. Software is executed with two hosts (HOST A and HOST B). The operation is performing in two phases.

Phase I: Without MAI

HOST A and Host B have a log file with size 230 Byte and 439 Byte respectively. In this case (without MAI) system have to transfer both log file with same size to controlling device. This means there 669 Byte (230 + 439) need to transfer to controlling device. This is shown in Table 1.Time taken by the system to transfer the file are 205 ms and 221 ms this is shown in Table 2.

Table 1. Log file size during the journey of mobile agent (without apply mobile agent intelligence)

Machine	Size of log file in Bytes
Controlling device	669
Host A	230
Host B	439

Table 2. Time taken by mobile Agent during return log file to controlling device without MAI

Machine	Time in ms
Host A	205
Host B	221

Phase II: With MAI

HOST A and Host B have a log file with size 230 Byte and 439 Byte respectively. Now MA analysis these log file and extract useful information to send back to controlling device. So now size of log file (after MAI-analysis) is 206 Byte and 405 Byte this is shown in Table 3. Table 4 shows that the Time taken by the system to transfer the file is 165 ms and 175 ms.

Table 3. Log files size during the journey of mobile agent (with mobile agent intelligence)

Machine	Size of log file in Bytes
Controlling device	611
Host A	206
Host B	405

Table 4 Time taken by mobile Agent during return log file to controlling (with mobile agent intelligence)

Machine	Time in ms
Host A	165
Host B	175

6. RESULTS ANALYSIS

It is clearly despite with the experiment that the size and time of log file need to transfer to CD is larger in Phase 1. IDS with MA intelligence shown in Phase 2 give better performance. Figure 6 and Figure 7 shows the graph difference between size and time before applying mobile agent intelligence and with applying mobile agent intelligence respectively.

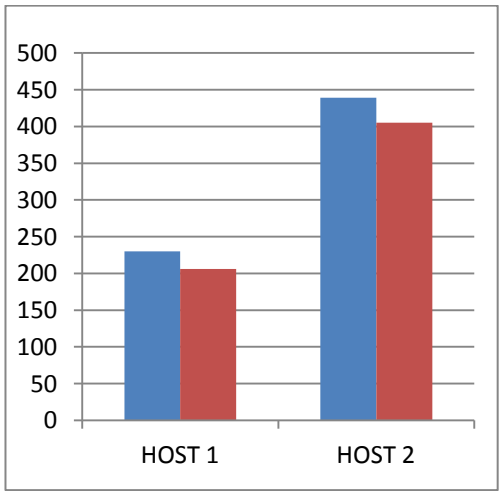

Figure 6: Difference between size without and with MAI

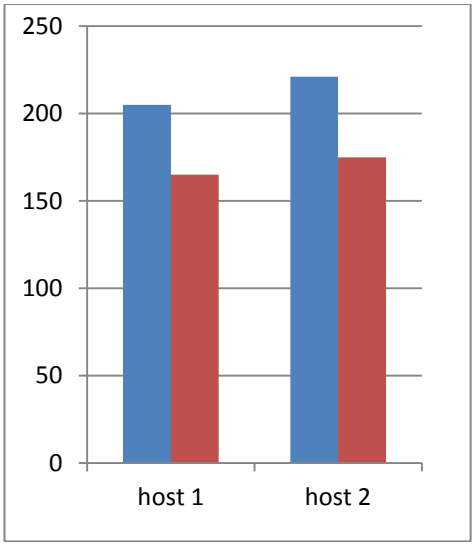

Figure 7: Difference between time without and with MAI

7. CONCLUSION AND FUTURE WORKS

This work introduced new IDS with mobile agent intelligence that increase the overall performance .The main idea behind this mechanism of architecture is to reduce the log file size. RMI establishes a good environment for mobile agent systems that allows the mobile agents to visit new places during a journey. Some time hosts may be configured with the invalid configuration of the web log file and not acceptable to store them .this architecture can help in this situation. According to architecture, the mobile agent system detects the proper configuration of the web log file implemented by using RMI in java language. Two experiments have been performed and according to the result, proposed architecture proved its efficiency in reducing the mobile agent size and time.

As future work and to take advantage of this architecture, this architecture with RMI method can be implemented in several existent mobile agent systems that put the assumption of architecture in their consideration. So, we can measure the benefits of architecture and no doubt it will open new approaches to enhance mobile agent models.

ACKNOWLEDGMENT

I would like to acknowledge and extend my heartfelt gratitude to Mr. Vivek Tiwari, Researcher (PhD) at Maulana Azad National Institute of Technology (MANIT-Bhopal), for their expertise, stimulating suggestions, experience and encouragement in all the times of research period.

8. REFRENCES

[1] Priyanka Patil1 and Ujwala Patil," Preprocessing of web server log file for web mining", World Journal of Science and Technology 2012

[2] Usman Asghar Sandhu , Sajjad Haider , Salman Naseer, Obaid Ullah Ateeb," A Survey of Intrusion Detection & Prevention Techniques ",2011

[3] Nisha Verma, Mohd Husain, Manoj Kumar Shukla," Research on Mobile agent based network intrusion", 2011

[4] Mueen Uddin, Kamran Khowaja and Azizah Abdul Rehman," Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents", 2010

[5] V. Tiwari, S.K. Lenka & S. Gupta.(June-2010)," Performance Evolution of Java Remote Method Invocation and Mobile Agent Techniques in Context of Distributed Environment" IEEE International Conference on Networking and Information Technology (ICNIT 2010) Manila, Philippines, IEEE Catalog Number:CFP1023K-PRT, ISBN:978-4244-7577-3.

[6] V. Tiwari & S. Gupta" *Computational Study of .NET Remoting and Mobile Agent in Distributed Environment*" International Journal of Computing, Volume 2, Issue 6, June-2010, ISSN: 2151-9617.

[7] Fakher Ben Ftima, Kamel Karoui, Henda Ben Ghezala, "Misconfigurations Discovery Between Distributed Security Components Using the Mobile Agent Approach", ACM New York, NY, USA 2009

[8] Bhushan Trivedi , Jayant Rajput , Chintan Dwivedi and Pinky Jobanputra," Distributed Intrusion Detection System using Mobile Agents", 2009

[9] Omar Abouabdalla, Homam El-Taj, Ahmed Manasrah, Sureswaran Ramadass," False Positive Reduction in Intrusion Detection System: A SURVEY", 2009

[10] Sergio Ilarri, Eduardo Mena, Arantza Illarramendi, "Using cooperative mobile agents to monirot distributed and dynamic environments", Elsevier Science Inc. New York, NY, USA 2008

[11] Álvaro Herrero, Emilio Corchado, María A. Pellicer, and Ajith Abraham, Hybrid Multi Agent-Neural Network Intrusion Detection with Mobile Visualization, 2007

[12] Yong Joon Park , Jae Chul Park ," Web Application Intrusion Detection System for Input Validation Attack", IEEE Computer Society Washington, DC, USA 2008

[13] Dalila Boughaci1, Kamel Ider2 and Sofiane Yahiaoui," Design and Implementation of a Misused Intrusion Detection System Using Autonomous and Mobile Agents" ACM 2007

[14] Pradeep Kannadiga and Mohammad Zulkernine," DIDMA: A Distributed Intrusion Detection System Using Mobile Agents",2005

[15] Shao-Chun Zhong', Qingfeng Song', Xiao-Chun Cheng, Yan Wang', A Safe Mobile Agent System for Distributed Intrusion detection, 2003