Sindh Univ. Res. Jour. (Sci. Ser.) Vol.43 (1-A) 01-04 (2011)

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

A Profiling Model on the top of Agent Collaborative Environment to Monitor Suspicious Activities

G.A. Mallah[1], N. A. Shaikh[1], Z. A. Shaikh[2] and M. Shah[3]

[1] Computers and Emerging Technologies , Shah Abdul Latif University, Khairpur
[2] Computers and Emerging Technologies FAST-National University, Karachi
[3]Lancashire Business School, University of Central Lancashire, United Kingdom

e-mail: noor.shaikh@salu.edu.pk, zubair.shaikh@nu.edu.pk, mhshah@uclan.ac.uk

*Corresponding author: G.A. Mallah, e-mail: ghulam.ali@salu.edu.pk,

Received 12 th May 2011 Revised 13th June 2011

Abstract: The profiles of all insiders in the organization are built and maintained in the proposed model to identify threat. Software agents are autonomously working to record all activities of the authenticated users. When profile is matured, it is compared with the policy of the organization and insider's profile is marked as acceptable or suspicious accordingly. The model is generic, adaptable and can be deployed most of the organizations without changing its code. Manager agents and the Profiling agents have been designed for implementation of the model. Profiling agents trace all activities and behavior of the authenticated employees and send to the Manager agent for necessary processing for its analysis. The decision is taken at the Manager Agent end to avoid any threat.

Keywords: software Agents. Insider Threat, Profiling , Behavior Monitoring, Network Security.

INTRODUCTION

The problem of Insider Threat has been addressed in this paper and the Profiling is the proposed solution for that. The fundamental definition of profiling is to monitor the activities of an employee within an organization. During investigation and implementation of the vulnerability assessment model it is learnt that insider threat is in fact a giant dilemma where both technology and user behavior must be addressed. Yet in the existence of sophisticated expertise network remains insecure because of capricious human behavior that is always threat to the organization. Therefore in a corporate environment user's behavior must be monitored to know the actual personality. There is always need to know what user really is doing in the organization, whether user is going beyond limits or working within the policy of the organization. There is need to observe whether user is focusing on the prime responsibility or wasting time and money of the organization. A complete profile of a user and an autonomous approach to handle it is needed to achieve the goal. Profiling for security through software agents is the solution that is presented in the paper. At low level, organizations are using different kind of technology, protocols, procedural security measures, but an agent based autonomous system at high level is needed for profiling to monitor user activities in an organization (IBM, 2009).

MATERIAL AND METHOD

Addressing following questions will support to build an efficient model against insider threat. For example the activities that a user is performing in the organization, are in accordance with organization's policy or not? Whether user's behavior is normal or suspicious? Whether user is certified to do so or not? Whether user is crossing limitations or remains within them? Whether user comes into view from the particular machine or coming from other machines too? How much someone is destructive for the organization? The ACENET scores every user of the organization and maintains a detailed profile. It is really hard to determine whether a legitimate user is doing anything malicious activity. Expectantly such activity would stand out as strange when compared to the user's routine behavior. This kind of theory was available but not done experimentally (Mallah, and Shaikh, 2004).

The proposed model is adaptable and can be easily deployed in any corporate environment. At application layer any agent can be designed within a shorter period of time on user demand because the abstraction has been provided; only behavior of the agent is to be defined. Agents have been designed as service on the top layers of the agent framework. The available agents create profile of the user and start

monitor activities autonomously. The threats have been categorized and for each category agents have been designed to monitor behavior of the users. The architecture is capable to adopt any given policy in accordance to any organization (Wanli and Sharma, 2009).

Agent and the execution environment are main factors of this model where agents operate to solve the problem through predetermined and learning based routines. The model is developed package to provide suitable environment over computer networks where various agents can live and perform other activities autonomously. Moreover, these agents can communicate with each other as well. At higher level this communication takes place just by message passing but internally socket based communication is underway. The agent designing is based on the classification of server and client side environment. The proposed model is shown in **(Fig. 1)**.

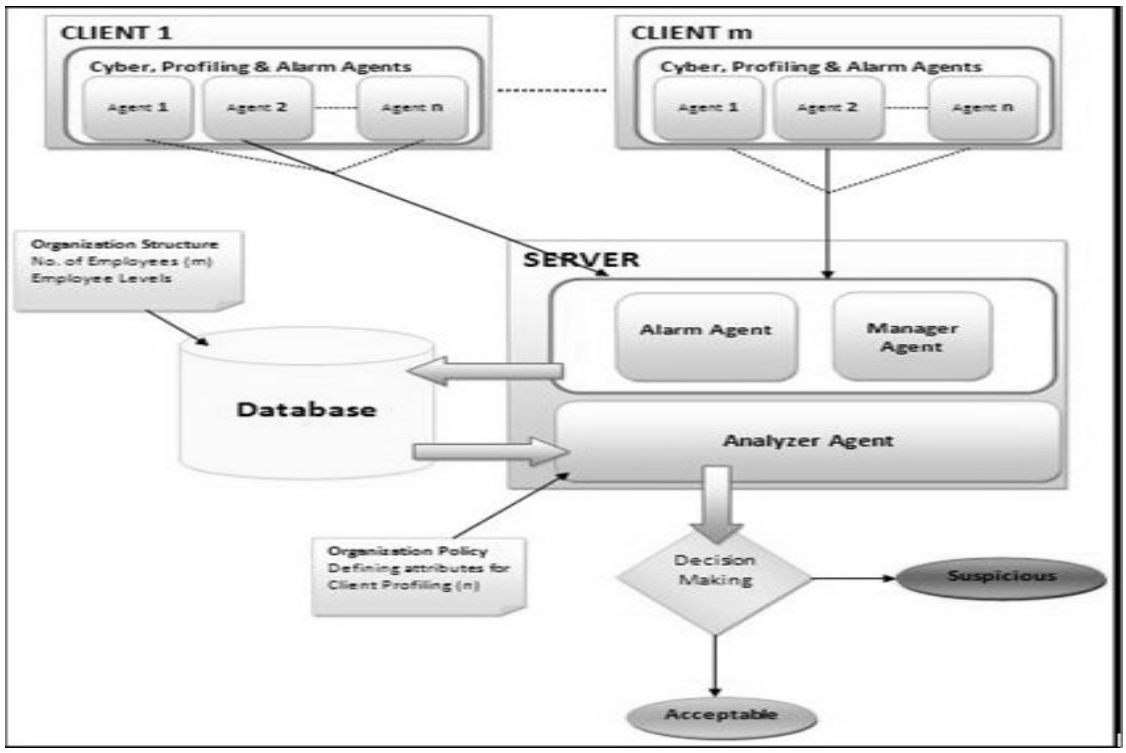

Fig 1: Proposed Profiling Model with various agents

RESEARCH METHODOLOGY

The description and activities detail of the agents running over ACENET is given below.

A. Server-supporting agent designing

These are the agents that reside on the system administrator machine and manage the framework across the network. Currently three kinds of the instances (agents) are developed:

i) Manager Agent

A powerful and most efficient agent that receives the messages from client agents and forwards to the database in the view of predefined organizational policy. It performs multiple insertions actively and maintains the database date wise.

ii) Alarm Agent Server

Alarm Agent is in fact an idea of designing agents on client's requirement to generate alerts in case of severe threat. Organization's policy will decide the sensitivity of the most harmful action of the insider user. For example if organization defines external device attachment as the major violation, then the alarm agent is capable to get an image of that activity from the client agent and propose immediate response to that.

iii) Analyzer Agent

The third key component of server side agent is capable of reading the data from database and transforms them into reportable form for viewing of the administrator. This agent is supportive as it could provide decision support for the organization through its analysis.

B. Client-supporting agent designing

These are the agents that remain active on client end. They get activated right at the moment when any one logins the machine and starts work and some of them instantiated on trigger predefined to them. Three kinds of the instances are given below:

i) Profiling Agent

This agent keeps monitoring the non-cyber activities performing by the logged machine and forwards towards the manager agent. The monitored activities contain running processes, applications, system login, logout time, removable media usage, printer usage etc. This agent actually governs a set of agents who are dedicated to perform specific tasks indicated with their names. These agents are: Active application monitoring agent, Process monitoring agent, Session monitoring agent, Print activities monitoring agent, and Removable storage monitoring agent, etc.

ii) Cyber Agent

This agent keeps the track of all visited websites from the machine and sends them towards the manager agent in order to put them into the database.

iii) Alarm Agent Client

This dynamic agent is activated when user violates some sensitive rule of the organization. Therefore it is named as online monitoring. This agent sends screenshot at the instance when user performs most threatening activity. Backend database is used to keep the record in manageable form as it could be analyzed and even predict in future.

To generate and maintain profile of the activities of all users browsing is assumed as the main source. Browsing has been further divided into windows resources browsing and internet resources browsing. What and how the resources of the systems and network have been visited. These activities will be monitored: Login and Logout time, Processes or applications, the shared resources access (files, printers, folders), Time to time Screenshots of the user's machine will be taken as evidence, Printer usage and External device in or out. Internet browsing activities of the users will also be monitored (Branigan, 2009).

When user logs into the system, the agents get initiated and start transmitting the data towards server side management agents. Management agents establish placing the data into the database and hence analyzer agent prepares reports available for the web reporting. In fact, overall system functioning is accomplished by means of system profiling, cyber, and alarm agents. They capture and monitor the behavior of the users from all machines, time to time, and transmit towards the management agents either in routine or at any particular event. On the other hand the manager agents keep on inserting the data into the database for the analysis of it by analyzer agent (Hinson, 2008).

The design follows service-oriented architecture. The design may lead to any maximum limit of internal security assurance and more flexible as it can be scheduled in accordance to any organizational level. The service oriented architecture could be scheduled in accordance to any organizational policies in order to classify the behavior of its users it also additionally facilitates the alarming functioning to prevent the organization from some harmful activities in short it is the perfect and scalable product that has been developed as research product and could be brought to any limit of implementation within domain of user profiling environment (Mallah, *et al.,* 2008).

RESULTS AND DISCUSSIONS

To check whether framework is producing right or wrong results, having a valid dataset is very important. For insider threat rare dataset is available therefore there is need to test results on the real data produced in any organization. Datasets specific to the insider threat are merely available. No one can deny the importance of developing and validating insider threat models (Caltech, 2007). True Positive, False Positive, True Negative and False Negative are four values that will be result of any evaluation. , The normal behavior is classified as normal then it is a true positive; in the same way if there is no normal behavior and that is actually not normal then it will be called true negative. False negative and false positive are errors, where false positive implies the rejecting a hypothesis that should have been normal and false negative means the error of accepting a hypothesis that should have been rejected (Mallah, *et al.,* 2010). 300 positive and 100 negative instances have been taken to check results **(Shown as Table-1**). All calculations are shown as equations 1~3.

TP = 268	FP = 07
FN = 32	TN = 93
300	100

Table 1: Positive and Negative Instances

True Positive Rate (TPR) of the framework is calculated as:

$$\left[\begin{array}{l} TPR = \dfrac{TP}{TP + FN} \\ = \dfrac{268}{268 + 32} \\ \\ TPR = 0.89 \end{array}\right] \quad (1)$$

False Positive Rate (FPR) will be calculated as:

$$\left[\left[\begin{array}{l} FPR = \dfrac{FP}{TN + FP} \\ = \dfrac{07}{93 + 07} \\ \\ FPR = 0.07 \end{array}\right]\right] \quad (2)$$

The TPR and FPR of the framework are 0.89 and 0.07 respectively.

$$\begin{array}{l} NPV = \dfrac{TN}{TN + FN} \\ = \dfrac{93}{93 + 32} \\ = 0.744 \end{array} \quad (3)$$

The results of the framework were tested in two categories, one category with a suspicious (threat) the other category with a normal behavior. There are always unusual chances to examine a perfect separation between the two groups. Indeed, the distribution of the test results will definitely overlap. False positive and false negative are Type-I and Type-II errors respectively. In this model Type-I errors have been focused instead of Type-II that indicates that the behavior is appeared as threat while it is normal.

CONCLUSIONS

ACENET framework has been developed and its components have been discussed in detail. The framework is still in development phase therefore we also call it as model. This model generates and updates users' profiles to avoid and detect insider threat. Vulnerability assessment and the profiling model have been discussed in the previous chapters that provide foundation to the model where various research experiments were done with different agent platforms and evidences have been provided to support the claim. It was also concluded that user-profiling to monitor activities of the user can be used to detect and avoid insider attack. Agents play pivot role to create and maintain the profiles of the users that are presently applied to detect threat and in future calculate the threat level to avoid it. The proposed model supports distributed environment to solve distributed kind of applications. The model follows the renowned agent standard of FIPA as agents modeled on other platforms can interact with the agents developed on the proposed model.

ACKNOWLEDGEMENTS

This paper is extended version of our own work accepted in International Conference on Computers and Emerging Technologies (ICCET 2011), held on 22-23 April 2011 at Shah Abdul Latif University Khairpur Mirs, Pakistan.

REFERENCES

Branigan, S. (2009) "High-Tech Crimes Revealed: Cyber war Stories from the Digital Front", July 2009.

Caltech (2007) Dataset Archive, 2007, available at http://www.vision.caltech.edu/html_files/archive

Hinson, G. (2008) The Value of Information Security Awareness, CISSP CISM CISA MBA CEO, IsecT Ltd. Updated September 2008.

IBM (2009) "Stopping insider attacks: How organizations can protect their sensitive information", Report, September 2009.

Mallah, G.A., N. A. Shaikh, and Z.A. Shaikh, (2008) "Towards an automated Multiagent system to monitor user activities against insider threat", published in proceedings of International Symposium on Biometrics and Security Technologies, ISBAST 2008, held on 23-24 April 2008, 01-05, appeared in IEEExplore.

Mallah, G.A., N.A. Shaikh, and A.W. Shaikh, (2010) "A Research Survey of Software Agents and Implementation Issues in Vulnerability Assessment and Social Profiling Models", published in Australian Jour. of Basic and Applied Sciences, 4 (**3**): 442-449.

Mallah, G.A. and Z. A. Shaikh, (2004) Vulnerability Assessment through Mobile Agents–An Analysis, Design and Implementation", presented and published in E-Tech 2004 Conference held on 31st July 2004 organized by IEEE.

Wanli and D. Sharma, (2009) A Multiple Agents Based Intrusion Detection System", Knowledge-Based Intelligent Information and Engineering Systems: 9th International Conference, Australia, 205-211, Sep. 2009.