Australian Journal of Basic and Applied Sciences, 4(5): 851-858, 2010
ISSN 1991-8178

Result Analysis and Performance Evaluation of ACENET through Confusion Matrix Technique on Standard Dataset

[1]Noor Ahmed Shaikh, [1]Ghulam Ali, [2]Madad Ali Shah, [3]Zubair A Shaikh

[1]Shah Abdul Latif University, Khairpur
[2]Sukkur Institute of Business Administration
[3]National University of Computer & Emerging Sciences, Karachi

Abstract: The ACENET, first FIPA compliant agent framework over. NET to provide facility of abstract programming to agent oriented programmers, deployed over corporate network to monitor behavior of the users to generate and maintain profiles to avoid insider threat. Agents running over framework are intelligently performing their tasks in backend and become activate as users log into the system. According to local needs of the organizations the agents have been created to gather information of various activities inside organization. This paper presents brief overview of what and how developed framework monitors the behavior. The importance of organization's policy has been discussed where weight-age has been assigned to profile attributes to identify threat contribution of each suspicious activity. The performance of the model has also been evaluated on the basis of specified parameters based on confusion matrix technique. Finally collected results have been analyzed to match with the targeted objectives.

Key words: Agent framework, Insider Threat, Performance Evaluation, ACENET, User profiling

INTRODUCTION

An Agent Collaborative Environment on .NET (ACENET) was designed on the top of .Net that follows FIPA, the well known agent standard owned by IEEE, so that the developers may create and integrate complete distributed agent applications. There are many reasons to choose .Net framework, few of them are discussed here. .Net is a emerging technology, widely used by maximum users, supports many programming languages and is excellent web supporting technology (Ali, G., 2009). This significance of this work is that though 100+ agent platforms are available commercially and academically but not a single platform exists on .Net. that follows FIPA standard (German, E. and L. Sheremetov, 2008). This is first ever effort in this domain where agent oriented programmers commence to work on the framework as the high level application developer may explore agents in such a rising technology. Parallel to this ACENET is first .Net based fault-tolerant agent platform that provides a decentralized architecture by implementing separate communication layer among different machines (Mallah, G.A. and Shaikh, A Zubair, 2007). After successful designing of ACENET, its implementation has been focused to get targeted results. Addressing the problem of insider threat, there are some research questions that need to be answered after deployment of the framework. For example Where, when and who attached the external device into the machine for where the usage is prohibited? Which websites have been accessed by the users inside organization and with what frequency? What activities user performed from the unallocated machines?

Focusing these points may cause many advantages. One can harm the network resources by running some threats, viruses or destructive processes, so framework can keep the track of executed applications. The time wasting activities that are normally prohibited in the organizations such as chatting, running media player, etc can also be monitored to avoid wastage of time, the historical profile of users will specify if the time spent for a particular session matches their normal behavior. A divergence will increase the belief on suspicious behavior (Chris, D. and C. Holte, 2006).

2 Policy and Profile Attribute Weightings:

To estimate the level of overall threat to the organization each individual activity threat has been assigned weighting (Credant Technologies, 2007). The maximum threat level to the organization has been set up to 1.

Corresponding Author: Noor Ahmed Shaikh, Shah Abdul Latif University, Khairpur
E-mail: noor.shaikh@salu.edu.pk,

In order to bring the monitored activities into quantifiable form, threshold limits have been set to estimate the behavior of the user. Fig-1 shows these threshold weightings.

Various studies and the policies defined by the organizations are showing that all threats are not of the same level and weightings. External devices particularly flash drive has been ranked as the major source of data leakage and is identified as the maximum threat to organizations (Buckland, M., F. Gey, 2009). Due to the reason, reputable organizations do not allow the usage of flash drive for in and out of data. Policy defines threshold values and it is obvious that policy does not remain static (Bisson, M., 2009). Addressing this problem the policy has not been hard coded in the framework hence provided in XML format to avoid restructuring and rewriting of the entire code. These weightings may vary depending upon their significance inside the organization according their policy.

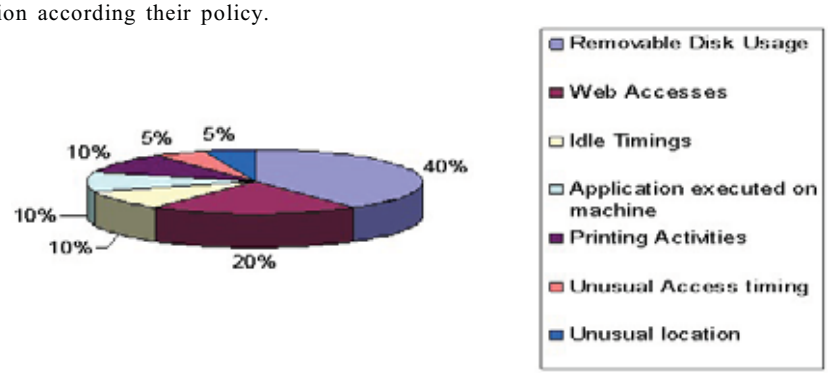

Fig. 1: Organization's policy showing threat percentage of the activities

2.1 Description of Weighting Allocations:

The profile attributes in form of activities have been taken into certain rules based on their nature. Nevertheless, each rule is not valid for every one like variety of privileges for various people within the organization. Hence each rule in various levels has been categorized and every user is associated with a particular level showing the authorities vested in the user by the organization corresponding to the position. Binary and gradient are the conventions used as the policy, discussed in the previous chapter. The policy and threshold will be compared with the profile of the employee to compare how much deviation is there. All results have been taken and analysis has been done on the basis of the policy specified.

Increment policy for specified users is applied until the maximum limits of corresponding activities, specified in the above table. The total threat will not exceed threshold that is stated by the organization. This activity monitoring approach is applicable for every user inside organization. To calculate threat level, a logical separation of the organization into three zones is proposed. The proposed zones are called High alert zone, Alert zone and Normal zone. The threat level to the organization will be identified through the value of Y. $Y = \sum Xi / n$, where n is the number of users, Y represents a zone and it is a function of Xi.

In order to visualize the clear difference for the threat level y-axis has been distributed into following zones:

Normal zone ranges at 0
Alert zone ranges between 0 – 0.5
High alert zone ranges between 0.5 – 1.0

If value of $Y > 0.5$ then organization is assumed to be in High alert zone and necessary actions will be required to stabilize the situation. If value of Y is between 0 and 0.5 then organization is assumed to be in Alert zone, because there is a big chance of its shifting into High alert zone, therefore it also requires high monitoring. If value of Y is equal to zero then it signals that everything in its normal state.

The threat level of an individual user to the organization will be identified through the value of X.

Calculation for $X = \sum aj$, where $j > 0$ and $j < 8$ with detail of a1 = activity1 weighting to the a7= activity7 weightings.

Xi represents individual user of the organization, while aj represents threat level of individual activities. The maximum threshold value for aj is 1. If values of X for any user becomes 1, that shows that the user is maximum threat for organization and may cause severe losses. Figure 1 shows the weighting percentage of each threat in the organization according to the policy.

2.2 Performance Evaluation:

The performance of the framework has been evaluated on self-generated dataset. The datasets are collected from various types of the organizations that fall into the categories of static (Fixed practices, fixed size), dynamic (Fixed practices, variable size) and adaptive (Variable practices, variable size).

The standard model for performance evaluation is given below.

If predicted outcome is p and the actual value is also p, then it is called a true positive (TP); whereas if the actual value is n then it is called a false positive (FP). On the other hand, a true negative will always appear when probable outcome and the actual value are n, and false negative is when the probable outcome is n while the actual value is p (Ali, G., 2009). To determine whether an insider is really threat to the organization, the possible outcome of the developed framework will be: If threat exists then the behavior of the user is SUSPICIOUS, otherwise NORMAL.

Mapping above model on our framework will justify in the way that the case will be true positive (TP) if an insider's probable action is suspicious and the actual action is also suspicious; however the case will be a false positive (FP) if the actual action is normal. Conversely, a true negative (TN) will occur when both the probable outcome and the actual action are normal, and false negative (FN) is when the probable outcome is normal while the actual action is suspicious. The four outcomes of the framework can be devised in a confusion matrix as given in table-I.

Table I: Confusion matrix to detect insider user behavior

Predictive Behavior	Observed Behavior	
	Suspicious	Normal
Suspicious	True Positive (TP)	False Positive (FP)
Normal	False Negative (FN)	True Negative (TN)

The results are calculated from 50 positive and 50 negative instances

TP = 46	FP = 03
FN = 04	TN = 47
50	50

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

$$TPR = \frac{TP}{TP + FN}$$

$$= \frac{46}{46 + 04}$$

$$TPR = 0.92$$

False Positive Rate (FPR) will be calculated as:

$$FPR = \frac{FP}{TN + FP}$$

$$= \frac{03}{47 + 03}$$

$$FPR = 0.06$$

Various model performance metrics can be derived from the confusion matrix, given above. The mainly used metrics is accuracy (ACC) that can be defined by formula:

$$ACC = \frac{TP + TN}{TP + TN + FP + FN}$$

$$\frac{(46 + 47)}{100}$$

$$ACC = 0.93$$

The TPR, FPR and the ACC of the framework are 0.92, 0.06 and 0.93 respectively.

The specificity is generally calculated to find proportion of negative cases correctly predicted as negative where as high specificity defines a low Type-I error. Specificity can be calculated as under.

$$Specificity = \frac{TN}{TN + FP}$$

$$or$$

$$1 - FPR$$

$$\frac{47}{47 + 03}$$

$$or$$

$$1 - 0.06$$

$$= 0.94$$

The calculated specificity of the framework, i.e. 0.94 shows that there is low type-I error.

The Positive Predictive Value (PPV) is used to calculate the proportion of cases predicted positive which are correctly predicted. For information retrieval, positive predictive value is known as precision and measures the fraction of documents returned that are relevant.

$$PPV = \frac{TP}{TP + FP}$$

$$= \frac{46}{46 + 03}$$

$$= 0.938$$

The Negative Predictive Value (NPV) is calculated to know the proportion of cases predicted negative which are correctly predicted. In terms of conditional probability, it is the probability that a case is truly negative given it is predicted negative.

$$NPV = \frac{TN}{TN + FN}$$

$$= \frac{47}{47 + 04}$$

$$= 0.921$$

The predictive values, 0.938 and 0.921, PPV and NPV respectively, show that framework gives better results for positive and negative instances, i.e. suspicious and normal behaviors.

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 (Paulo, C., 2000). 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.

3 Results and Analysis:

Usually results are taken through various simulation techniques but the beauty of our framework is that the results have been collected through real environment with the deployment and testing of academic version of ACENET. The advanced technology and tools of .Net framework at frontend and backend have been installed to get real results. The necessary reports have been generated through Microsoft's tools. The framework produces and maintains a profile consists of all observed activities. It compares with the threshold

values to decide the type of the user behavior. Table-II shows the observed and the threshold values that were obtained during testing of the framework.

Table-II: Threshold and observed values against activities

Activities	Threshold	Observed
Removable Disk Usage	0.4	0.4
Web Accesses	0.1	0.05
Idle Timings	0.1	0.1
Application executed on machine	0.1	0
Printing Activities	0.1	0.05
Unusual Access timing	0.2	0.1
Unusual location	0.15	0
Total	1	0.7

The observed value of an individual in table 3 is 0.7 out of 1.0 that alarms that the threat level of the individual has been entered into the high alert zone, i.e. maximum threat for the organization. Following figure reflects table-II representing multiple bar diagram for comparison of the observed and threshold values against activities.

Now let us consider overall organization situation through Y. As discussed earlier that Y is the trust rating of an organization that can be monitored on daily or weekly basis in order to visualize the trend of organization and its trust zone. Let us have a demonstration on some data for a week.

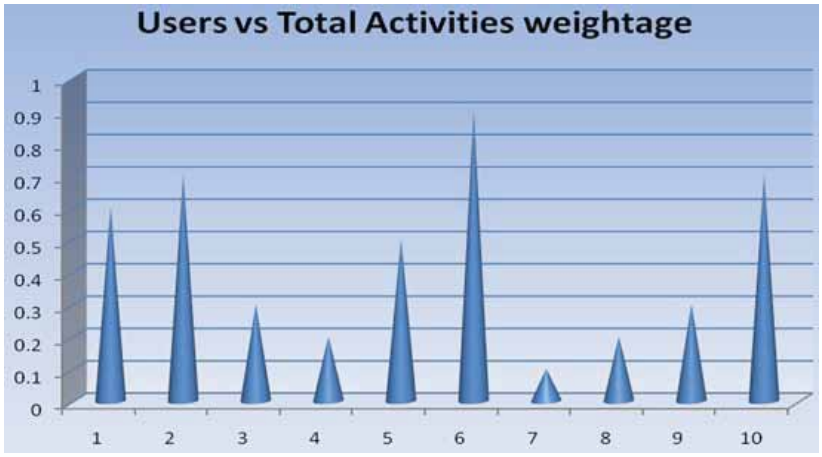

Fig. 2: The contribution of users in threat

The above graph shows that none of the users is in the normal zone (at zero level), 6 users are in Alert zone (at 0.1 – 0.55 level), while 4 users are in the High alert zone (at 0.6 – 1.0 level).

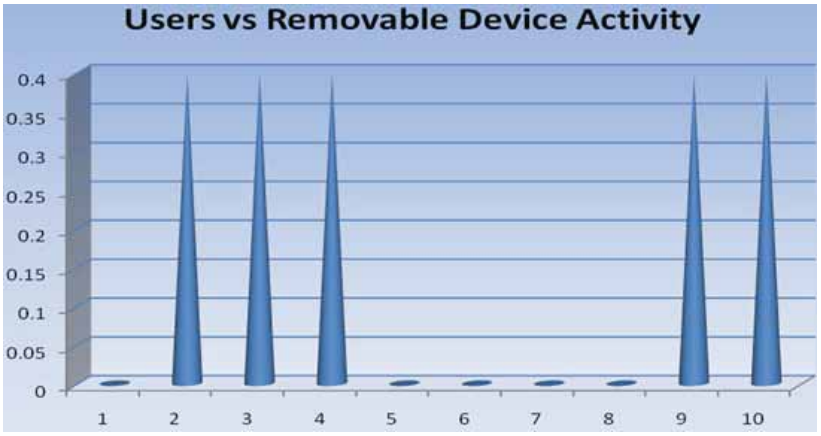

Fig. 3: Users' activities regarding usage of external device

Fig-3 shows the threat of activity-1 (attachment of the removable device) in the organization. According to the policy of the organization the type of threat of the activity-1 is binary. User is either allowed to use device or not. If an unauthorized user plugged flash drive there will be increment of 0.4. The maximum value of this activity is also 0.4. The graph shows that 5 users are violating the policy and the threat level of all 5 users is highest, i.e. 0.4, because of binary level. The threat will not go beyond 0.4. The question here arises what will happen if a user plugs flash drive more than once. The answer is simple; as this threat is severe according to the policy of the organization therefore an agent is there to report online and alarm to get immediate attention.

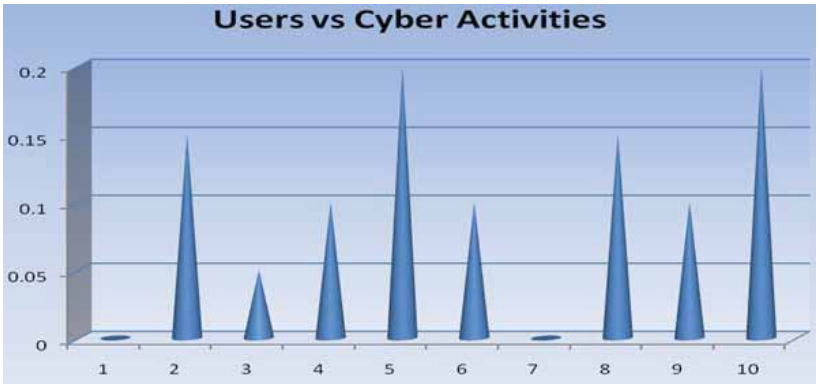

Fig. 4: Users' activities regarding cyber access

Fig-4 presents the threat of activity-2, web access, in the organization. According to the policy of the organization the type of threat of the activity-2 is gradient. If a user uses restricted websites then there will be increment of 0.025 after every 15 minutes. The maximum value will be 0.2 that will alarm that user is becoming 100% threat in this particular activity. The graph shows that 8 out of 10 users are violating the policy where 2 of them have reached to the maximum level of the threat and remaining are going towards the maximum (Sheldon, F., 2009).

The graphs for all activities are shown in the above format that helps in the analysis the profile to measure the threat level. Following graph shows the profile of the specific user to analyze the deviation from the organization's policy.

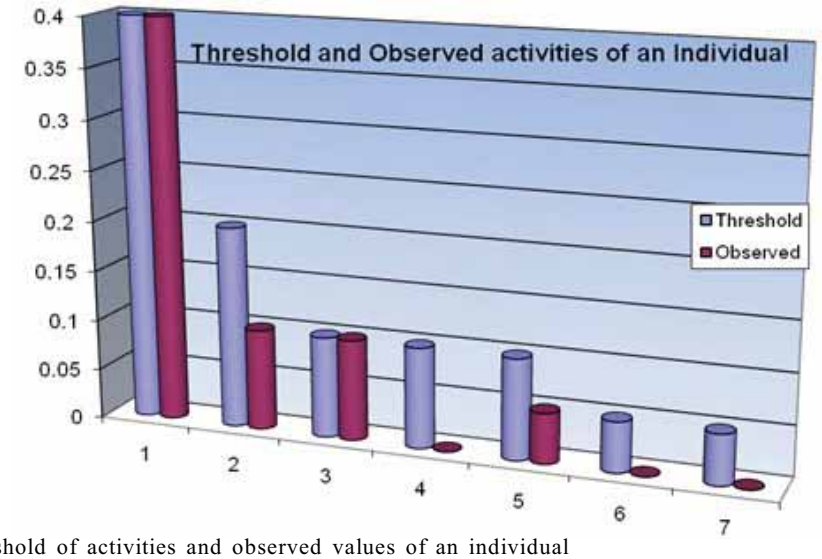

Fig. 5: Threshold of activities and observed values of an individual

The threshold activities in fig-5 show the maximum threat level, while observed activities represent the behavior of a user regarding all seven activities. The graph shows that this particular user violated the policy

of the organization in four activities. It also alarms that user has reached at the maximum level of the threat in activities 1 and 3. The individual has violated the policy in activities 2 and 5 but not reached at the maximum level. The numbers from 1 to 7 on x-axis represent the activities discussed earlier in a table. The profile can be calculated and represented as the value of X as discussed earlier. In the above case the value of X is 0.65. As said earlier if value goes beyond 0.5 then it alarms that the user has been entered into high alert zone. The alarming agent will alarm the situation (Jigang, X. and Q. Zhengding, 2007).

4 Conclusion:

It has been concluded that along with the deployment of the framework there is need of understanding the business process and a clear policy of the organization that will be a threshold to monitor overall behavior of the users. The developed framework follows agent standardization models and provides following features:

- Launches user profiles based on historical data and actual practice
- Monitors all online and offline activities of the users during whole session
- Identifies suspicious behavior through threshold comparing
- Forecasts the maximum risk level
- Stops possible exploitation through generating alerts
- Logins at unusual times and locations
- Illegal process and applications execution
- Illegal access to prohibited websites
- Long and short time stay in the organization
- Illegal use of external devices
- Wastage of time in the organization

The results in the framework have been taken on the windows operating system and the protocol hierarchy, but in future there is need to consider and deploy it over variety of operating systems.

ACKNOWLEDGMENT

This work has been done at Center for Research on Ubiquitous Computing (CRUC), FAST - National University Karachi under guidance of Professor Dr Zubair A Shaikh, Director FAST-NU. The research was financed by Higher Education Commission, Islamabad through Indigenous PhD scholarship.

REFERENCES

Ali, G., N.A. Shaikh, Z.A. Shaikh, 2008. “Towards An Automated Multiagent System To Monitor User Activities Against Insider Threat”, published in International Symposium on Biometrics and Security Technologies, ISBAST 2008, 23-24: 1-4.

Ali, G., N.A. Shaikh, Z.A. Shaikh, 2009. “Agent-based User Profiling Model for Behavior Monitoring”, published in 2009 International Conference on Future Networks Proceedings, pp: 3-7:

Ali, G., N.A. Shaikh,, Z.A. Shaikh, 2009. “A Decentralized and Fault-Tolerant FIPA-Compliant Agent Framework based on .NET”, submitted to Mehran University Research Journal.

Buckland, M., F. Gey, 2009. “The relationship between recall and precision”, Journal of the American Society for Information Science, 45(1): 12-19, John Wiley & Sons, Inc. New York, NY, USA publishers.

Bisson, M., B. Behncke, Neri, Marco, 2009. “LiDAR-based digital terrain analysis of an area exposed to the risk of lava flow invasion”, Journal: Natural Hazards, Publisher Springer Netherlands, 50(2): 321-334.

Chris, D. and C. Holte, 2006. “Cost Curves: An Improved Method for Visualizing Classifier Performance”, Machine Learning, 65(1): 95-130.

Credant Technologies, 2007. “iPods and Other Portable Storage Devices Are a Growing Threat for Data Leakage in the Workplace”, Dallas.

German, E. and L. Sheremetov, 2008. “An Agent Framework for Processing FIPA-ACL Messages Based on Interaction Models”, Lecture Notes in Computer Science, Publisher Springer Berlin / Heidelberg, pp: 88-102.

Jigang, X. and Q. Zhengding, 2007. “Bootstrap technique for ROC analysis: A stable evaluation of Fisher classifier performance”, Journal of Electronics, Publisher Science Press, co-published with Springer-Verlag, 24: 523-527.

Mallah, G.A. and Shaikh, A Zubair, 2007. "The Design and Implementation of an Agent Framework to Support Distributed Problem Solving", published as Lecture Notes in Electrical Engineering Book of Springer-Verlag.

Paulo, C., 2000. "DTB Project: A Behavioral Model for Detecting Insider Threats", A project of Advanced Research and Development Activity (ARDA), supported by US Navy.

Sheldon, F., R. Abercrombie, Mili, Ali, 2009. "Evaluating security controls based on key performance indicators and stakeholder mission", published in Proceedings of the 4th annual workshop on Cyber security and information intelligence research, ACM New York, NY, USA publishers.