A First Step towards Reducing Insider Threats in Government Organizations

1Maaz Bin Ahmad, 1Muhammad Fahad, 1Abdul Wahab Khan 2Muhammad Asif

1Department of COCIS PAF-KIET Karachi, Pakistan;
2Department of Electrical Engineering CUST University Islamabad

Summary

The problem of insider threats is one of the most challenging to the organizations and research community since a long time. It is well proved that the damage done by insiders is more severe than that of external attackers .In government organizations, most of the users are not aware of the advanced security measures so are more vulnerable to such kind of attacks. As observed by reviewing many case studies of insider attacks, it is clear that insiders normally perform some unusual or suspicious activities before launching actual attacks. So monitoring these activities and taking proper actions in time is helpful to avoid such kinds of attacks. In this paper a risk assessment methodology is presented to compute the threat levels of users in lesser IT literate environment. This methodology is an extension to our previous work [1]. The difference is that in previous work the approach was for pure IT related business organizations where most of the users were aware about the security measures. The methodology combines technical measures and psychological indicators to detect insiders. The simulation of methodology in a test network against different scenarios shows that it efficiently categorizes users according to their threat level. So it provides a useful first step towards categorizing the users according to their actions.

Keywords:
Insider; Organization; Risk; threat; psychological

1. Introduction

Normally the organizations may face many threats which may be categorized in to external threats and insider threats. The external threats are easier to handle then internal threats. Several mature means are available to detect or prevent the external threats, like firewalls, IDS (Intrusion detection system), access controls etc. The issue of insider threats is more fatal because of the unique characteristics of insiders. Insiders usually know a lot more about organization and security policies which are being implemented there. Also they usually have more privileges and trust of the organization than external attackers. So if one of your trusted employees (who also have privileges) behaves as an insider attacker, then he can damage the organization a lot more than an external attacker. So this issue requires lot of efforts to be done to handle it properly. Normally the detection methodologies for insider threats are geared towards detecting the insiders once he/she has launched an attack. The drawback in these methodologies is that damage is already done by the insiders. So a method should be there which may gives us a hint about the possible threats which insider may pose in the future. In this paper a methodology is presented which assigns threat score (TS) for all users inside the organization. Threat score is computed by taking in to account different actions performed by a user, his behavior analysis and by analyzing the vulnerabilities in the system/machine assigned to him. The proposed methodology works on the principle that only having capability to attack does not mean the presence of risk until intents are also there to attack. The methodology is geared towards government organizations where most of the users are not well trained IT professionals and thus suffer more from these types of attacks.

Section 2 of the paper provides an overview of the work done by researchers in this area. Section 3 provides proposed methodology followed by analysis and implementation in section 4. In section 5 conclusion and future directions are presented followed by references.

2. Related Work

CERT [2], [3] proposed a guideline for detection and prevention of insider threats. In these suggestions it was emphasized first to identify the organization level risks, which is not an easy task to do. Since the scope of insider is very broad i.e. ranging from the legitimate users to vendors, analysts and service providers. So an organization-wide risk assessment process should be there to handle it. Then the policies of the organization should be clearly and consistently documented. It helps in removing some of the insider threats. The selection of proper words like must or should helps to accomplish this task.

There should be a security awareness culture developed among the employee of the organization. This can be achieved through security training programs conducted for the employee. The output of this is that employee would be aware of the fact that there may be threats present either from inside or outside to the organization. The employee should be screened before hiring them. It helps

Manuscript received June 5, 2016
Manuscript revised June 20, 2016

to observe any abnormal behavior. The process of pre-employment, employment and termination should be carefully reviewed by the organization so that the negative issues like termination should be well managed. It is necessary because the research says that most of the information sabotage issues arise after the termination. Physical environment security is also important in this regard. The access attempts should be logged and reviewed time to time in order to identify any violation to the physical security policies. Also there should be strict passwords and account management policies among employee, contractors and sister organizations. Enforce the rule of least-privilege among employee and others according to their role so that only those resources should be available to an employee, which are needed by him to accomplish his role. It is also recommended to incorporate the issue of insider threats in the SDLC (software development life cycle), since the vendors or third party software may have back doors or covert channels for insider threats. So this process of developing software should be monitored. The unauthorized changes in the system should be controlled, and it should be the part of mitigation strategy of insider threats. Also the actions of the employee should be logged, monitored and audited to identify any suspicious behavior. Since the employees know that they are being monitored, so the insider would try to access the system remotely. The problem can be more severe if the remote access of a terminated employee was not disabled. So it should be handled properly and the computer access should be deactivated after termination. The secure backup of critical information and resources should be there for an organization because no organization can completely prevent insider threats. If insider attack is launched then there should be a response plan to be executed. Cappelli et al [4] proposed the development of new tools which would be available to the organizations in order to analyze risks and to mitigate threats. Cultural, technical and procedural factors of organization need to be taken into account to accurately assess the risks in case of insider threats. Einwechter [5] proposed that the combination of host-based intrusion detection scheme and network based intrusion detection scheme (HIDS NIDS) can be used to detect the insider threats. So he took a right step in the right direction to mitigate the insider threat problem. But there are some serious problems with this approach. Insiders may disable or can interfere with the IDS because they know the system very well. Carl [6] discussed several issues like outsourcing process as a mean of launching insider threats as organizations normally fail to control the access and privileges to the outsourced organizations. His solution emphasized to monitor human factor, education, awareness and to develop such security controls which may work in different environments. Viega et al [7] presented a framework to promote a security aware culture inside the organizations and also explained its use. But not a really practical approach was explained in it. SANS [8] presented a risk scoring methodology incorporating the best practices as suggested by CERT. It is closer towards practical implementing risk assessment methodology but its assumption is that the organization is a pure IT business one so most of the users are well educated about security threats. In [11] several risk to U.S critical organizations were discussed along with suggestions how to mitigate those. Yet the real practical way to implement those was missing.

3. Methodology

In this methodology, we observed and analyzed different unusual behavior and activities of insiders to guess his intent which helps in minimizing the chances of possible insider attacks. We computed the threat score (TS) for each employee based upon different metrics (discussed below). It should be noted that TS value would be an integer. Now we see how to assign TS value to each employee.

$$TS = F_{attributes} + F_{behavior} + F_{vulnerability} \qquad (1)$$

Where Fattributes represents the key features of the employee, Fbehavior represents the behavior of that employee and Fvulnerability represents the vulnerabilities in the machine or computer used by that employee. Since Fbehavior reflects more about the malicious intent of any employee, it is given more weight-age i.e. 60. Fattributes is given max weight of 15, while Fvulnerability is given weigh 25. Thus the value of TS for each employee would lie between 0-100. Now we see what features of employee and/or machine he/she is using should be considered to find values of all these Fs.

a) $F_{attributes}$: User physical and electronic privileges of using or changing organizations resources and information system will serve as a base to assign value to this function. Examples of some of the attributes are user rights to O.S files, user access to commercial critical files, user designation and role in the organization, user access to printers/scanners and user physical access to the critical resources of the organization. So different users would have different value of this function but once assigned, that value would remain more or less static. Max possible value of this function is 15 while max possible value of each of the five attributes is 3. For example, users physical access to critical re-sources attribute is assigned a value 3 if a user has unlimited access to many resources, 1.5 if user may have some limited access and 0 if user may have never access to such resources.

b) $F_{behavior}$: This function is very important since its value reflects more accurately about user malicious intents and it may change with the passage of time. Factors which contribute to assign this value are as follows:

User competence: It reflects about the user knowledge and skills about computer. Max value of weight of this subcategory may be 25. For calculating this value we have divided users in three classes:

Class A: In this class there are users which have higher technical designation and who are using system for a period of more than one year e.g. system admin., network admin. software engineer etc.

Class B: All those persons who are using system for a period more than one year and are not related to computers technology belong to this class.

Class C: Non- technical users using system for less than one year belong to this class.

Variety of knowledge and intensity of knowledge: Variety is calculated by counting number of unique applications executed by user in a given time and is given max value 10 while intensity of knowledge is guessed by the above mentioned categories of users and is given max value 15. So, based upon these a weight is assigned to each user ranging from 0-25. Also the CPU and RAM utilization and parallel running applications by each user are monitored which helps to as-sign weight to intensity of knowledge sub-category of user competence factor. For example, if a user executed more than 12 unique applications in an hour then variety value would be 10, if more than 6 unique applications were executed in an hour then diversity value would be 10 otherwise a value of 3 is assigned. Also, if the user belongs to class A, then a value 10 is assigned to intensity of knowledge sub category, if user belongs to class B then a value of 6 is as-signed otherwise a value of 3 is assigned to this sub-category. If any users CPU and RAM utilization and number of concurrent application running exceeds by the allowed ones for his category then a value of 5 is added to intensity of knowledge sub category for that user.

User Network operations: Total number of active connections, Total amount of data transferred, data transferred per connection, total amount of data transferred per session etc. is calculated and compared against the max threshold values of these metrics and accordingly weight is assigned to this category. Values lie in the range of 0-15.

User interactions with honey files: These are the files having luring names and information to a malicious intent insider. Constant monitoring of these files helps us to identify the intent of a user. Whatever he/she does with these files e.g. open, delete, modify, rename etc. is logged. These files contain dummy data and information but for an insider attacker it looks real. So by observing his/her behavior regarding these files we can deduce what would he/she do if he/she finds a chance to sabotage the organization. Based upon his/her activities, suspicious level of that user is changed and a weight is assigned. It is to be noted that these don't give us indication of an actual attack but helps us to separate a malicious intent user from a normal one. C file watcher mechanism is used to obtain log of such activities. A weight value ranging between 0-10 is assigned to this category depending upon operations performed on these files. For example deleting and/or modifying operations carry more weight than opening or viewing operations.

User psychological data: To collect data for it, we developed a questionnaire to assess the anger/depression [9],[10] of an employee. The stats about insider attacks say that majority of the insider attacks have been launched by angry or unsatisfied employees. The reason of his/her anger may vary a great deal from not satisfied with management behavior, not satisfied with his pay, may have some economic problems, not rewarded his/her hardworking, not promoted on a post which he/she deserved, is overburdened, received warning letter on such a small mistake etc. So the questionnaire is designed to have an idea about any issues he/she has regarding his/her job in the organization. Resolving such issues in time may help us to remove the chances of a possible attack. Each user has to fill that questionnaire electronically on bi-weekly basis. Though, the user can give wrong statements, but the questionnaire is designed in such a way that it would be easily known whether he is lying on not. This is done by cleverly mixing the questions with such questions whose answers are already known to the management. Also the previous history of the employee regarding his/her misbehaving and/or abusing the resources of the organization is also observed which helps to as-sign appropriate weight to this module. This category is assigned a max possible weight value of 10. Max possible value of 60 is assigned to behavior function.

c) $F_{vulnerability}$: Logs obtained from our developed vulnerability assessment application are assigned a weight ranging from 0-25 according to the vulnerability condition of the system and user. We developed this application using C which performs vulnerability assessment of client's machine. This application runs as a service and gives information about no. of open ports on client machine, whether updates for O.S have been installed or not, right service pack is installed or not, O.S firewall is active or not, whether antivirus installed or nor, how many days passed since last up-dates of antivirus, are there any illegal processes running on this machine? O.S security manager is present or not etc. So by knowing this information appropriate weight is assigned to each client's machine. So at the end, a value of TS is assigned to all users which reflect the threat level he/she may pose in the near future.

4. Implementation and Discussion

We converted our C application for risk assessment in to a windows service and run that service on each of the machines in test network of seven nodes. We simulated three user types one manager, second data entry operator and third one was clerk, each having two nodes and different privilege levels. The users carried out their normal activities for the period of one week to have different threshold values e.g. for average CPU and RAM utilization, ports opened, average network connections per session, data transferred per session etc. Once the model was trained, one user from each category was advised to perform illegal scenarios. After every two minutes the results were obtained in terms of TS value (including separate values for all three functions) of each simulated user and alarm was raised based upon the resulting value. The user psychological data application was installed on server and users were asked to complete that form whenever it was required. Since this value doesn't change rapidly so users were asked to fill that form on bi-weekly basis. Each time some of the questions were updated and analyzed in detail to adjust TS value for each user. We defined rules to get the threat level of each user in all the scenarios e.g. if TS>60 then level is high, if TS<50 then level is low otherwise the level is medium. As a proof of concept we take some example scenarios to validate our approach.

A. Example 1

Henry was a manager in a water planning department of the government. He was annoyed due to his lower pay scale and wanted to damage the organization but didn't know how to do it. He downloaded several malicious software in order to accomplish his desire. His web interaction increased and captured by the sub-module of our application. His anger was also reflected from the suggestion form he filled. Also the security condition of his machine was not up to date due to his ignorance from necessary security updates. All of these factors were captured by different sub modules of the application thus resulted in increase in overall TS.

B. Example 2

Carl was a clerk in some power sector department of the government. His normal duties were to manage files and reports related to the department. He was annoyed from his managers due to their insulting behavior and decided to sabotage the organization. Due to his limited knowledge he didn't know how to do it effectively. He started to upload heavy confidential files on some social media. This activity was caught by the network interaction module of the application. Also he tried to misuse the login information in the honey files of the application which also increased his TS. Psychological assessment module of the application also captured his desperation. So the overall effect was that the application declared him as a very high risky user hence detected accurately.

User Category	User Type	Fatt val	Fbeh val	Fvul val	TS val	Lev
Clerk	N	9	22	15	46	low
Clerk	M	9	43	15	62	high
Manager	N	13	32	11	56	Med
Manager	M	13	50	11	74	High
Data Entry	N	6	16	18	40	low
Data Entry	M	6	30	18	54	Med

The example of the summary of results obtained in some of the scenarios [12] is presented in the Table I. As shown in the Table I, alarms were raised for the clerk and manager malicious activities. It is shown that malicious data entry opera-tor was not detected as having high threat level. The reason is obvious because he doesn't have much privilege, so he can attack within his limit thus making the overall TS value below the threshold of high level. It should also be noted that normal system manager was detected as having medium threat level. It is so because super system users may damage the organization a lot more than any other user can. So it is advisable to keep monitoring their activities all the time. We may offline analyze more activities of all the users having high or medium threat level to reduce false alarms problem. So this methodology proved as a good one to be applied as first line of defense in case of insiders. Note that it doesn't replace the actual detection methodologies but complements them. So we can apply this methodology in combination with other detection schemes in order to further analyze the activities of users having high or medium threat level and to minimize false alarms. Another advantage which it provides is that we can use non-uniform monitoring processes for different users according to their TS values. We may collect more data about activities of medium and high threat level users only. So it may help in reducing the overall processing overheads also.

5. Conclusion & Future Directions

A risk based detection methodology is presented for insiders in government organization who not only gives an idea about possible attacks but also helps to reduce the overhead involved in uniform monitoring processes. Its significance is clear because we can stop the attacks before being launched by using it. This when combined with strong detection methodologies can give us improved results to reduce the damage of insider attacks. A fuzzy based mechanism should be there after this module in order to properly categorizing the users so that different measures can be taken for different categories. Also there should be a strong prevention mechanism which should prevent the users from taking illegal activities.

References

[1] M. B. Ahmad, S.Rehman, A. Akram and M. Asif. Towards a Realistic Risk Assessment Methodology for Insider Threats of Information Misuse. Frontiers of Information Technology (FIT), 2014, Islamabad. Pages 176-181.

[2] CSO magazine. E-Crime Watch Survey. CSO magazine Summary, 2005. http://www.cert.org/archive/pdf/ecrimesummary05.pdf.

[3] CSO magazine (2006, 09, 6). E-Crime Watch Survey. CSO magazine 2006. http://www.cert.org/archive/pdf/ecrimesurvey06.pdf

[4] Cappelli, M. Dawn, Moore, G. Akash, P. An-drew, Shimeall, J. Timothy,Weaver, A. Elise, Willke, J. Bradford. Management and Education of the Risk of Insider Threat (MERIT): Mitigating the Risk of Sabotage to Employers' Information, Systems. Technical note, March, 2007.

[5] E. Eugene Schultz. A framework for understanding and predicting insider attacks. Compsec, London, 30 October 2002.

[6] Carl Corwill. Human factors in information security: The insider threat. Who can you trust these days? Information security technical report Science direct 2010.

[7] A.D. Viega and J.H.P Eloff. A framework and assessment instrument for information security culture. Computer and Security journal, Volume 29, Issue 2, March 2010, Pages 196–207.

[8] Balaji Balakrishnan. Insider threat mitigation guidance, SANS Institute InfoSec Reading Room, Oct 2015.

[9] BehaviorAssessment. www.cdc.gov/ncipc/pubres/pdf/YV/CDCYV SecIII.pdf

[10] ADULT ANGER VERSION 1.0 SHORT FORM. A brief guide to the 8-item PROMIS Short Form v1.0 Anger 8a. www.assessmentcenter.net/.../PROMIS%20Scoring%20SF%20Anger

[11] Risks to U.S. Critical Infrastructure from Insider Threat. Homeland Infrastructure Threat and Risk Analysis Center. 2013.

[12] M.B Ahmad, A.Akram, S. ur-Rehman and M.H. Islam. Implementation of a behavior driven methodology for insider threats detection of misuse of information in windows environment. Information: An interdisciplinary journal. Pp .8121-8136, Vol.16, No.11, November, 2013.