AN ARCHITECTURE FOR DETECTION AND INCIDENT RESPONSE OF INSIDER CYBER THREATS

Rushal Chauhan
Asst. Prof., Universal College of Engineering & Technology, Ahmedabad, Gujarat, India

ABSTRACT: Host-based intrusion detection methods play an important role in developing an Intrusion Detection System (IDS).In this paper, we present a Incidence Response Architecture for detection of insider threats, which combines two approaches, which are digital forensics and anomaly detection via correlation. With the help of these approaches we can easily identify origin of attack and action performed by Insider attacker which can be used to monitor an environment for Insider Threat. The operational flow of the system describes the flow of the Proposed Architecture as well a show the sequences of the steps executed.

KEYWORDS: Insider Cyber Threat, Network Forensics, Reactive Approach, Proposed Architecture, Anomaly Detection.

I. INTRODUCTION

In the last few years, the Internet has experienced explosive growth. Along with the widespread evolution of newly emerging services impact of attacks has been continuously increasing as well. Usage of computer in an environment in such a situation incidents occur which involve internal users with malicious intensions. Such users commonly known as Insider Threats often exploit the technical & operational vulnerabilities in an enterprise network to illegally access ,modify, destroy confidential data .The insider threat has received considerable attention and is often cited as the most serious security problem. It is also considered the most difficult problem to deal with, because “insider” information and capabilities not known to external attackers[1]. Many previous studies have looked at the broad scope of the problem without any real attempt to identify a solution. Insider misuse in a broad range of application domains-for example, critical infrastructures, privacy-preserving database systems, financial systems, and interoperable health-care infrastructures [2].

The Insider can be defined as someone who possesses, namely in terms of someone with:

- Knowledge: Implies an open system, one that remains secure (if at all) even with full knowledge of the system operation; alternatively, security through obscurity;
- Trust: An individual is empowered by the organization to be an insider;
- Access: An insider is in possession of a credential giving access to the system-An IT centric perspective, since the system in general does not know who possesses the credential [2,3].

Current Approaches for Detection of Insider Threats:

Misuse Detection
Misuse detection is based on the knowledge of system vulnerabilities and known attack patterns[6].Misuse detection refers to the detection of intrusions by precisely defining them ahead of time and watching for their occurrences[5]. Misuse intrusion detection usually use methods of expert system, TCP/IP protocol analysis, and pattern matching[5]. It is possible to detect system behavior patterns corresponding to known attacks from audit trails, logs (status records), or changes in attacked system[6].A primary advantage of signature detection is that known attack can be detected fairly reliably[4].Secondary advantage of signature detection is protecting computer immediately upon installation[4]. Disadvantage of using this approach is it is required to define signatures for all possible attacks that an attacker may launch[4].

Anomaly Detection
It assumes that a cyber-attack will always reflect some deviations from normal patterns[7]. Expected system behavior is predetermined manually or automatically by prepared profile characterizing user/system behavior in the computer system[6]. Primary advantage using this approach is the ability to detect unknown attacks as well as “zero day attack” by using Statistical Anomaly Detection technique[4]. Secondary, Profiles of normal activity customized for every system, therefore it is very difficult for an attacker to know with certainty what activities it can carry out without getting detected[4].Disadvantage of using Anomaly detection is shown in poor performance, maintenance of the Profile also be time consuming[4].

II. RELATED WORK

In traditional systems, neither techniques nor approaches for detection of insider threat are included in the Host based systems. In addition, there is no such reactive technology or efficient architecture exist which effectively detect insider Threat in the Host based systems. In our Proposed Architecture, combination of traditional technologies plus forensic Analysis is used to show immediate results right after the incidence takes place within the environment.

In our Proposed Architecture, User Profile generated by Host Based Sensor is in XML format.

Why XML?

- In real world computer systems and databases contain data in incompatible formats.XML data is stored in the plaintext format.This provides software and hardware independent way of storing data. This makes it much easier to create data that can be shared by different applications.
- Xml is designed to transport and store data.
- In XML, data is stored in hierarchical format. Thus we can easily understand the hierarchy.
- XML is self-descriptive language. By using this we can quickly edit without using external editor.

Forensic is defined as things that can uniquely identify a person. The important thing and the major advantage regarding the forensics is the preservation of the evidence that is collected during the process. We performed the Digital Forensic Analysis, with the help of Windows Registry.

For a comprehensive list of Registry keys that directly relate to a computer Forensic examination by using document Registry Quick Find Chart.

List Item	**Location**
Access Programs	HCU\Software\Microsoft\Windows\Current Version \Explorer\User Assist
Removable Media	HKLM\SYSTEM\ControlSet00x\Enum \USBSTOR
	HKLM\SYSTEM\MountedDevices
Web Browser	HKCU\Software\Microsoft\Internet Explorer
Search History	HKCU\Software\Microsoft\ Internet Explorer\TypedURLs
Downloads	HKCU\Software\Microsoft\ Internet Explorer\Download Directory
Connected Computers	HKCU\Software\Microsoft\Windows\ CurrentVersion\Explorer\ComputerDescriptions
Recent Open Documents	Software\Microsoft\Office\10.0\Excel\ Recent Files
	Software\Microsoft\Office\10.0\Word\ Data
	Software\Microsoft\Office\10.0\Power Point\Recent File List
Recent Documents	Software\Microsoft\Windows\Current Version\Explorer\RecentDocs
Recent Executable Programs	HKCU\Software\Microsoft\Windows\ CurrentVersion\Explorer\RunMRU
	HKCU\Software\Microsoft\Windows\ CurrentVersion\Explorer\ComDLG32\ opensave MRU

Table1: Registry Quick Find Chart

III. PROPOSEDARCHITECTURE

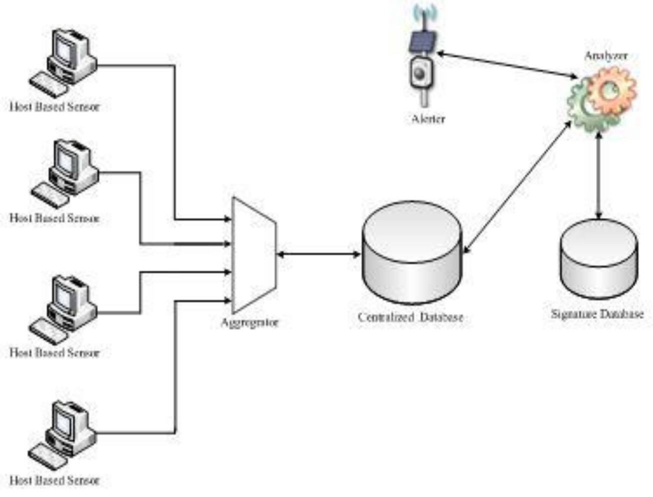

Figure 1: Proposed Architecture

In Proposed Architecture, There are four main components:

Analyzer:
System testing is based on data comparison with represented by correlation action with User Profile. Analyzer assign threat level of each User based upon the defined baseline threshold values. Analyzer will do pattern matching activity of User sample data which stored in Centralized Database and compare with the Signature Database. Signature Database contains predefined rules and signature of all users. By comparing with the Centralized Database, If Analyzer finds activities of user is deviated from its normal behavior by comparing baseline value with threshold value. If the vast deviation appears in User Profile, the activity is considered as suspicious activity. By detecting activity as suspicious, Analyzer increase the threat level of that particular user and send message to the Alerter.

Host Based Sensor:
One of the key techniques employed by the architecture involves host-level monitoring of user-initiated events.The sensor is designed to profile a baseline for the normal search behavior of a user.It senses the data from the host machine by using the help of Host Agent. The sensor installed by each Host machine monitored all registry-based activity, process creation and destruction, window GUI access. Sensor generatesUser Profile based ondifferent activities performed by the user. User Profiles are developed to easily and instantly find out anomalies and malicious accesses. After successful creation of User Profile,it will be delivered to Aggregator.

Aggregator:
Aggregator act as a collector. It is responsible for receiving different User Profiles through the Host Based Sensor and sends it into the Centralized Database for future references.

Alerter:

It provide interface to security expert to identify the activity based on the collected data which reside in Analyzer. The main purpose of the Alerter is generating the Alert message for the suspicious activities.

Operational flow of the system:

For the purpose of monitoring activities done by Host machine, it is required to install Host Agent on each machine .After that Host Agent will be activated and fetch details of the system such as System OS, Hardware details etc.. Host Agent generate a User Profile for particular host and fetch various information related to host such as Executable programs, Typed URL by user, most recently open/save files ,USB/Removable media, Network components from the windows registry. Virtually everything done in Windows refers to or is recorded into the Registry. The Registry is referenced in one way or another with every action taken by the user. After collecting information, Host Agent displays the User Profile and store into the database for future reference.

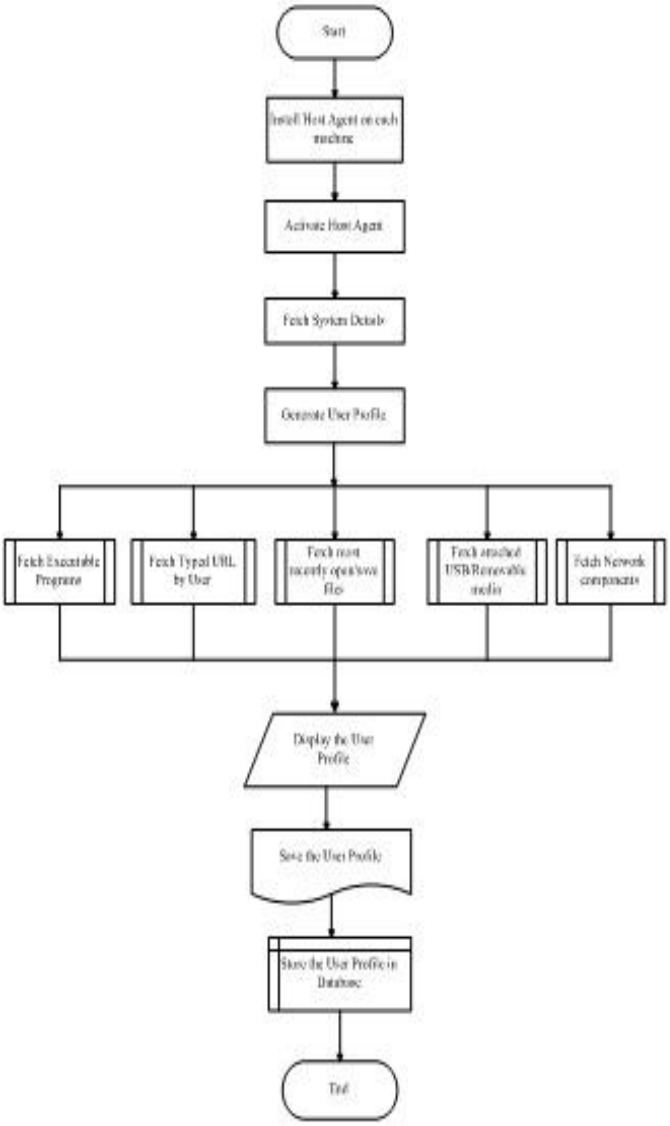
Start
Install Host Agent on each machine
Activate Host Agent
Fetch System Details
Generate User Profile
Fetch Executable Programe
Fetch Typed URL by User
Fetch most recently open/save files
Fetch attached USB/Removable media
Fetch Network components
Display the User Profile
Save the User Profile
Store the User Profile in Database
End

Figure 2.1: Operational flow of Host Based Sensor

After creation of different User Profile, Aggregator collect that profiles which is in xml format and encrypt the User Profile using SSL (Secure SocketLayer).Collector send this encrypted profile to the Centralized Database.

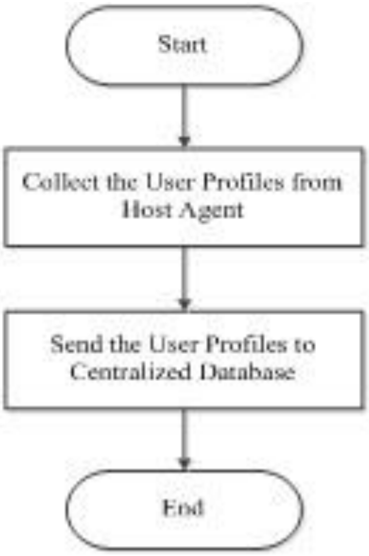
Start
Collect the User Profiles from Host Agent
Send the User Profiles to Centralized Database
End

Figure 2.2: Operational flow of Aggregator.

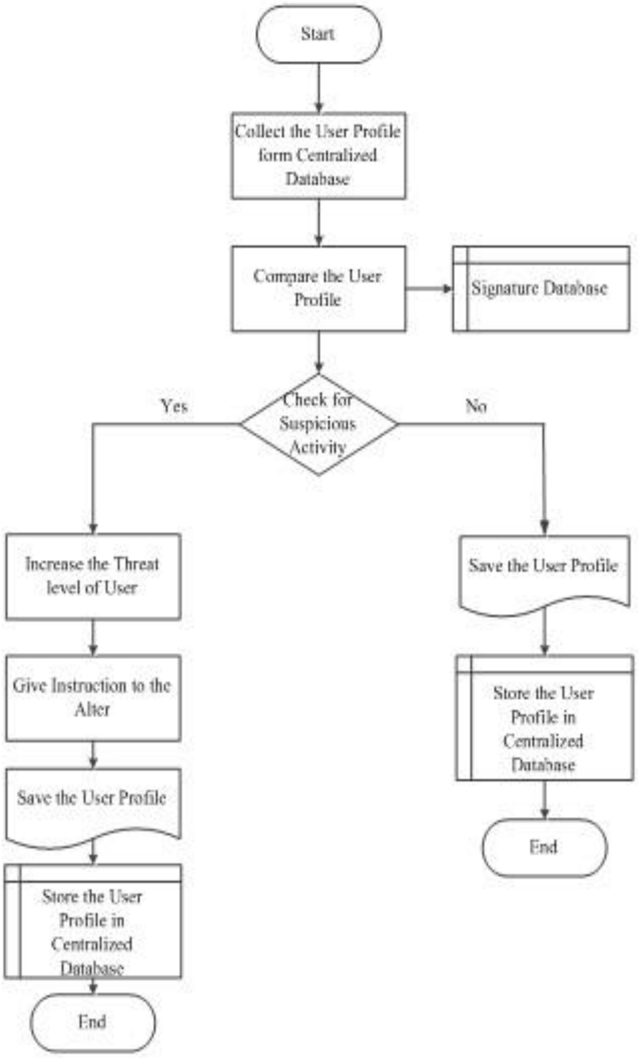
Start
Collect the User Profile form Centralized Database
Compare the User Profile
Signature Database
Check for Suspicious Activity
Yes
No
Increase the Threat level of User
Give Instruction to the Alter
Save the User Profile
Store the User Profile in Centralized Database
End
Save the User Profile
Store the User Profile in Centralized Database
End

Figure 2.3: Operational flow of Analyzer.

Analyzer will compare the User Profile which reside into the Centralized Database with Signature Database for check the activity is suspicious or not. Analyzer will do pattern matching and correlation of User Profile with Signature Database. If user activity is suspicious then Analyzer, Increase the threat level and give instruction to the Alerter. It stores the User Profile into Centralized Database.

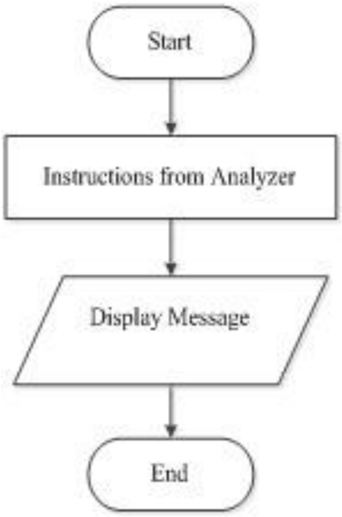

Figure 2.4: Operational flow of Alerter.

Based on the Analyzer instruction, Aleter display a message for suspicious activity.

IV. FUTURE WORK

The Host Based Sensor generates a User Profile which resides in the Centralized Database.Our future work includes the approaches to use the same User Profile as a baseline for detection of future attacks with the help of proactive monitoring and Machine Learning.

V. CONCLUSION

After analyzing different approaches for the detection of Insider Cyber Threats we have found out thatReactive Approach of the detection is the best for incident response and we have followed the same in our Proposed Architecture. In our approach, we have used combination of digital forensics and Anomaly Detection. With the help of our approach, it is possible to identify insider threats immediately after incidence has been occurred.

REFERENCES

[1]. Christion W. Probst atal. “Aspects of Insider Threats,”in Insider Threats in Cyber Security .SushilJajodia **,**Ed. New York:Springer,2010,pp.12-26

[2]. Peter G. Neumann. “Combatting Insider Threats,”in Insider Threats in Cyber Security .SushilJajodia **,**Ed. New York:Springer, 2010,pp 27-54

[3]. Matt Bishop at al. “A Risk Management Approach to the Insider Threat,” in Insider Threats in Cyber Security .Sushil Jajodia**,** Ed. New York:Springer, 2010, pp. 123-145

[4]. A.Patcha, J-M.Park, “Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends,” Computer Networks(2007),doi:0.1016/j.comnet.2007.02.001

[5]. L. Ying, Z. Yan, O. Yang-Jia ,“The Design and Implementation of Host-based Intrusion Detection System,” Third International Symposium on Intelligent Information Technology and Security Informatics,2010 ,pp.595-598.

[6]. L. Vokorokos, A. Baláž, “Host-based Intrusion Detection System,” 14th International Conference on Intelligent Engineering Systems , May 5–7, 2010,pp.43-47.

[7]. S. Singh and S.Silakari, “ A Survey of Cyber attack Detection Systems ,” IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.5, May 2009, pp. 1-10.