ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 2, March 2015

Detection of Anomaly Using Windows Registry Access

Kalyani Lokhande[1], Mona Batra[2], Mohini Sonawane[3], Bhavana Ingale[4]
BE, Department of Computer Engineering, SSBT's COET Bambhori , Jalgaon (M.S.),India[1,2,3,4]

Abstract— Security in network has become the most important issue. Many Intrusion system and anomaly detection system has been proposed, but they are primarily focused on misuse detection driven by signature or specification-based techniques. In this paper by using system identifications we are identifying and extracting potential outside users and their associated activities. We are using Windows Registry to identify the anomaly within our network, by using the combinations IP address, MAC Address, hard disk ID and Motherboard ID for the detection of anomaly. In this windows registry is treated as database which maintains the valid combination of identifications of the client. The client trying to access the network having identifications other than the address stored in the windows registry is treated as anomaly.

Keywords: **Anomaly, Windows Registry Access, IP Address, MAC Address, Motherboard ID, Hard disk ID.**

I. INTRODUCTION

Microsoft Windows operating system is one of the most popular operating systems, which is one of the most often attacked. Firewall is able to detect malicious access to the host, patches of operating system updates to fix the security holes that attackers exploit. These methods suffer from the drawback, therefore they are effective against discovered attacks, but are unable to prevent new kinds of attacks.

Network anomaly is an abstraction of existing intrusion detection techniques to the network level allowing us to monitor the security of multiple nodes and the network infrastructure too. Network anomalies refer to circumstances when network operations deviate from normal network behavior.

The anomalies can arise due to various causes such as bad configuration in network services and operating systems, network overload applications used by users, their effort to discover network and to gather information about it and its devices. An anomalous event known as surprising event. And the extent to which an anomaly is considered surprising is determined by the anomaly detector, on the basis of the probability of encountering the event.

Anomaly is a behavior based system which detects normal and abnormal users in system anomaly detection system establishes base line for all users and depends on it decides invalid user. Windows Registry is a database which stores configuration settings, options on Microsoft Windows Operating system containing the settings for lower operating system components and for applications which run on the platform that use the Registry.

II. LITERATURE REVIEW

Anomaly is a behavior based system which detects normal and abnormal users in system. So the process of detection of abnormal users is called as anomalies detection system & prevention of anomaly using the association rule is called Anomaly Prevention System. Anomalies detection system is a system for detecting computer anomaly and behavior by monitoring system activity and by classifying it as either normal or abnormal, after the classification denying that anomaly to return in the network.

Anomaly detection systems were first proposed by Denning as an integrated component with host-based misuse detectors and later implemented in NIDES to model normal network behavior in order to detect deviant behavior that may correspond against a network computer system to attack [5]. W. Lee described a framework and system for data mining, auditing and feature selection of intrusion detection models for the automatic computation. So the framework consists of classification, sequence analysis and link analysis for constructing intrusion detection models and host data or maybe applied to network data.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 2, March 2015

A variety of other work has appeared in the literature detailing alternative algorithms to establish normal profiles and applied to a variety of different audit sources. HNADP model which is used to detect and prevent the network anomalies using IP Gray Space analysis and MAC address filtering. This methodology is working in two phases first phase is identification phase and second phase is prevention phase [9].

There are various techniques have been applied to anomaly detection for detecting novel attacks like statistical analysis, clustering, support vector machines, many more. Although there's still a serious problem, high false positive rates, which make anomaly detection systems practically unusable [2].

The Using Hidden Markov Model in Enterprise Networks approach works at classifying the ARP traffic as an either abnormal or normal using a special HMM [5]. The main objective of this approach is to build an anomaly detection system, a model which is predictive and capable of identifying normal and abnormal behavior of network ARP traffic [5].

Although there are several other host-based intrusion detection and prevention systems, they are primarily focused on misuse detection driven by signature or specification-based techniques. As reality most Anomaly Detection Techniques attempts to set up normal activity profiles by computing various metrics and an intrusion is detected when the actual system behavior davits from the normal profiles [3].Comparison of the learning-based RAD to a number of commercial products that provide rules-based registry monitoring since to those systems which are unpublished.

The HNADP model detects anomaly using two phases: Identification of anomalous external host using IP gray space and relative uncertainty and Identification of category of Anomaly using dominant scanning port (DSPI).In this methodology, the protocol used is UDP and the database is stored in SQL. There is need to maintain Database manually. Another drawback is identification of anomaly is based only on MIC. There is no provision for how to handle IP spoofing and MAC spoofing [9].In our proposed system we have overcame this drawbacks by using Windows registry itself as a database and using additional system identifications.

III. PROPOSED SYSTEM

In Proposed system, we are detecting anomaly in network in client-server communication..

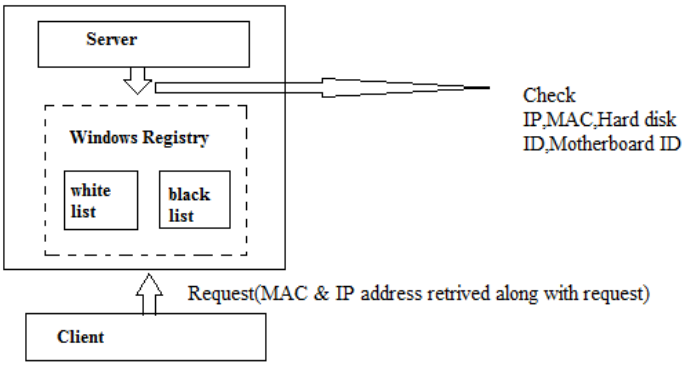

Fig 1: Working of Anomaly Detection using Windows Registry

In our project, the basic unique identifications are used they are IP and MAC address, hard disk and Motherboard ID. IP address is logical whereas MAC-address also known as physical address which uniquely assigned to each system .These addresses are retrieved from Windows Registry of client and compared with IP and MAC Addresses which are stored in windows registry of server. HKEY_CURRENT_USER which contains the root of the configuration information for the user who is currently logged on. The screen colors and user's folder's here the Control Panel settings are stored. So this information is associated with the user's profile. So this key is abbreviated as "HKCU".

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 2, March 2015

In today's world, authentication is based only on IP and MAC ID is not yet enough. Since, IP and MAC spoofing can be done. There are some unique identification that is Hard disk ID and Motherboard ID. If at all any of this unique identifications don't match, then also is treated as anomaly and blacklisted.
Here we are using two phases:

Phase-I Detection of Anomalies using Comparative algorithm

In this phase, when any client wants to get services by server then all the identification information is retrieved along with request .If combination of all four addresses matches then it is detected as white list client and allowed to access services. Otherwise, detected as an anomaly.

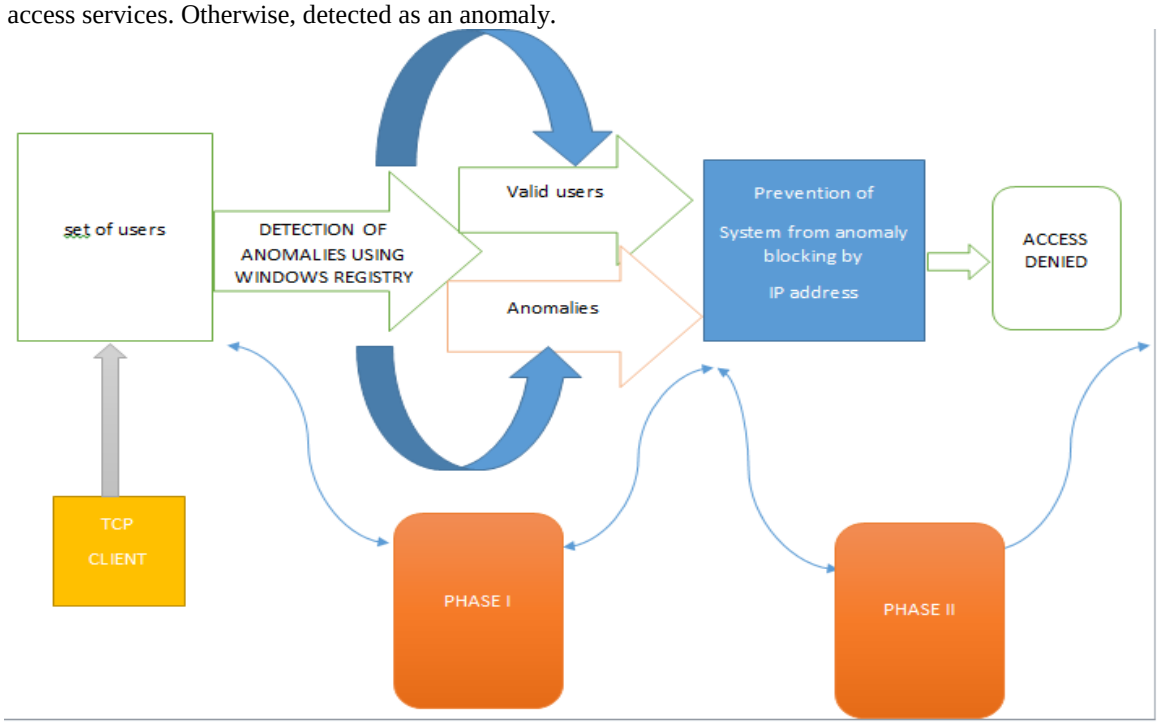

Fig 2: Anomaly detection and prevention

Phase-II-Prevention of Network from Anomalies using identifications

This phase processed the result of first phase. Once network anomalies detected then the working of this phase is starts. If any anomalous host interfaces out defended network then it becomes necessary to protect the network from such users. In this phase the system will check IP of client is already blacklisted. If so, this phase will deny all services of anomalous user.

IV. RESULT AND DISCUSSION

Client is requested to sever and server provides service to client but there may the case that the requesting client is not valid client. This invalid client is then acted as anomaly in the network and also affect the security of network. Therefore in our project we will identify the anomaly using windows registry system .In windows registry MAC address , IP address, Motherboard ID and Hard disk ID of valid client is automatically maintained. If there is case that invalid client stolen the IP address then due to MAC address invalid client is detected as anomaly, as invalid client MAC address is other than address store in windows registry system. Considering the case that the anomaly has done IP scooping as well as MAC scooping then also detected as anomaly, because windows registry contains the combinations as any of the combination is change the client is automatically considered as anomaly.

V. CONCLUSION

Security in network has been a major issue today. Security is not just about keeping people out of your network but also provides access into your network in the way you want to provide it, allowing the people to work together. Anomaly detection system using Windows Registry Access detecting anomaly using Identifications of system. The

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 4, Issue 2, March 2015

developed system works in fixed network environment. By using Client-Server communication scenario anomalies are detected by applying authentication algorithm.

In future by additional features and applying more sophisticated machine learning techniques to perform anomaly detection using behavioral analysis , we will try greater number of anomalies to capture advanced prevention technique.

ACKNOWLEDGMENT

At this level of understanding it is often difficult to understand the wide spectrum of knowledge without proper guidance and advice .Hence we take this opportunity to express our sincere gratitude to our respected guide **Mr. Nitin Y.Suryawanshi Sir** as a guide & Project In charge evolved an interest in our work and select an entirely new idea for project work. He has been extremely cooperative and helpful to us in sorting out all the difficulties. I would also like to thank our H.O.D **Mr. G.K. Patnaik Sir** all other members of our department who fully co-operated me during my project work. I would also like to thank **Mr. S. P. Shekhawat Sir**, Director of Academics and our principal **Dr. K. S. Wani Sir** for his warm support and providing all Necessary facilities to us.

REFERENCES

[1] Yogendra Kumar JAIN, Sandip S. PATIL "Design of Gaia Maselli , Luca Deri , Stefano Suin , "Design and Hybrid Network Anomalies Detection System (H-NADS) Implementation of Anomaly Detection System"2007 Using IP Gray Space Analysis" International Journal of Informatics Economic vol. 13, no. 2/2009 110.

[2] Y. Jin, G. Simon, K. Xu, Z.-L. Zhang and V. Kumar, "Gray" Anatomy: Dissecting Scanning Activities Using IP Gray Space Analysis". In Proc. of SysML'07, 2007.

[3] K. Jackson, Intrusion Detection Systems (IDS): Product Survey, Los Alamos National Laboratory.

[4] H. Debar, M. Dacier, and A. Wespi, Towards a Taxonomy of Intrusion Detection Systems, Computer Networks, 31(8):805-822, April 1999[4] Wei Lu, Mahbod T. and Ali A." Detecting Network Anomalies Using Different Wavelet Basis Functions", Communication Networks and Services Research Conference 978-0-7695-3135-9 IEEE August, 2008.

[5] Y.Yasami, M. Farahmand, V. Zargari "An ARP-based Anomaly Detection Algorithm Using Hidden Markov Model in Enterprise Networks", (ICSNC 2007), IEEE 2007.

[6] Xiuyao Song, Mingxi Wu, Christopher Jermaine, and Sanjay Ranka" Conditional Anomaly Detection", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 19, NO. 5, MAY 2007.

[7] Giulia Bruno, Paolo Garza, Elisa uintarelli, Rosalba Rossato," Anomaly Detection in XML databases by means, IEEE July 2007.

[8] Ricardo C. Carrano, Luiz C. S. Magalhães, Débora C.Muchaluat Saade and Célio V. N. Albuquerque "IEEE.

[9] Sandip S. Patil, Nitin Y. Suryawanshi "Detecting Network Anomalies using IP Gray Space Analysis and Preventing from it by using Machine Identification Code" International Journal of Computer Applications (0975 – 8887) Volume 34– No.4, November 2011.