International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 8, August 2016)

Enabling Efficient Data Sharing System using MAC IP (MIP) Level Intruder Filtering with Dynamic Alert and Logging System

Dr. Priti Mishra

Assistant Professor, Department of Information Science & Engineering, RRIT, Bangalore, India

***Abstract*-- "Ensuring distribution authentication for data sharing environment with multiple IDS and logging system" present the design of an advanced peer-to-peer file sharing Network. The focus of this is to analyze how far Network Technology can be used to detect new, unknown internal attacks and this gathers information about the hackers that can be used to improve the security of our network. Networks help to develop a reasoned, proactive response to a threat. This system ensures the peer authentication over the data sharing Environment. It provides multiple IDS with the aid of data security environment. Only Authorized client can access the files from server. If unauthorized client is trying to access the file from server. Then this system should be displayed only duplicate file contents, not from original files. Here data's are stored in Server which protects important files and directories. Internal intruder is blocked using IP and MAC filtering .IDS can protect important files and directories on our hard disk no matter what file-system type they reside on, anybody include root cannot change the files. Network IDS can also protect he important process from being killed.**

Today's Internet connected networks are under permanent attack by intruders and automated attacks of worms. A variety of detection tools exist such as Intrusion Detection systems (IDS) and firewalls, but the main problem is that they only react on reconfigured and therefore known attacks. Networks are an upcoming technology that can be used to detect and analyze network attacks. A Network is an apparently vulnerable system deployed to be hacked.

In this proposed system deals with multiple level of filtering the un authorized peer using login credential ,MAC ,IP filtering (MIP filtering) .An analysis of current Network approaches has been made and it has been evaluated in how far these approaches can contribute to the analyzation process. Some tests have shown that Networks are exposed to lots of known attacks and noise that hide the valuable information about new attacks and vulnerabilities. In this system main focus on data security as well IP level security using AES algorithm and IP vice versa. To implement this process developed using Java as Frontend and MYSQL as Backend.

***Keywords*-- RBF-route-based filtering, PAID-Probabilistic Agent-Based Intrusion Detection, IDS-intrusion detection system , NIDS- network based intrusion detection systems , HIDS - host based intrusion detection systems**

I. INTRODUCTION

A. Background

Intrusion Detection Systems are tools to assist in managing threats and vulnerabilities in this changing environment. Threats are people or groups who have the potential to compromise other computer system . These may be an inquisitive teenager, a discontented worker employee, or spy from an opponent company or any foreign government. Attacks on network computer system could be devastating, affect networks, and corporate establishments. Additionally, different disadvantages have been detected over using the current signature detection approach such as (Difficulties in updating information, unable to detect unknown novel attacks, maintenance of an IDS is necessarily connected with analyzing and patching of security holes, the attack knowledge is operating environment dependent, and the lack of information on user privileges and attack signature structure)[1].

An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. There are network based (NIDS) and host based (HIDS) intrusion detection systems. There are IDS that detect based on looking for specific signatures of known threats- similar to the way antivirus software typically detects and protects against malware- and there are IDS that detect based on comparing traffic patterns against a baseline and looking for anomalies. There are IDS that simply monitor and alert and there are IDS that perform an action or actions in response to a detected threat[2].

B. Motivation

The MIP filtering technique is to defend the attacks. The servers will use the hybrid peer to peer architecture to perform such kind of attacks. But, in the system, to introduce the secure system technique to defend such kind of malware attacks. So, it can avoid the malware attacks like internal theft attacks using the secure system.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 8, August 2016)

IP filtering is done at the project level, so if you have a staging server and a live page it might make sense to keep them in separate projects so that you don't have to keep turning IP filtering on and off. To access IP Filtering from the Home page, click Settings and then Privacy. In the field under Filter these IP addresses out of results, enter the IP(s) that you don't want to be counted in your experiment results. The IP filtering option lets you exclude as many IPs as necessary in a single line. Bear in mind that you should be using your public IP address[3].

MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. While the restriction of network access through the use of lists is straightforward, an individual person is not identified [3].

by a MAC address, rather a device only, so an authorized person will need to have a whitelist entry for each device that he or she would use to access the network. MAC filtering is also used on enterprise wireless networks with multiple access points to prevent clients from communicating with each other. The access point can be configured to only allow clients to talk to the default gateway, but not other wireless clients. It increases the efficiency of access to network [5].

II. Related Work

Recently, different studies have been presented to describe the architecture and the implementation of techniques for detecting and manipulating the spoofing activities over LAN. However, researchers such as explained the Probabilistic Agent-Based Intrusion Detection (PAID) system. These systems provide cooperative agent architecture, which can perform specific intrusion detection tasks (e.g., identify IP-spoofing attacks). PAID allow to other agents to share the probability distribution of an event occurrence [3].

A study presented a framework to investigate the prospective adaptive and cooperative defense mechanisms against the Internet attacks. The suggested approach is based on the multi agent modeling and simulation. This framework represents the attack as interacting teams of intelligent agents that act under some adaptation criterion. They adjust their configuration and behavior in compliance with the network Conditions and attack (defense) severity[1].

However, a study reported the design and evaluation of the Clouseau system, with the route-based filtering (RBF). This design was an effective and provide practical defense against IP spoofing.

Since RFB process critically customize on the accuracy of the IP layer information that used for spoofed packet detection. The inference process as described by them is "resilient to subversion by an attacker who is familiar with Clouseau"[4].

Another study proposed an ANTID scheme for detecting and filtering DDoS attacks which uses spoofed packets to circumvent the conventional intrusion detection schemes. This ANTID intends to complement the conventional schemes by embedding in each IP packet a unique path fingerprint that represents the route an IP packet has traversed; ANTID is able to distinguish IP packets that traverse different Internet paths[3].

III. MIP System

A Overview

The current IDS used two intrusion detection approaches firstly; anomaly detection approach, that used to manipulate the relation between profile and the current behavior of the TCP/IP, also determine the difference between profiles and detect possible attack attempts. Secondly; signature detection approach, used to detect ambiguous and unclear actions by analyzing and describing the action patterns such as (time, text, password etc).

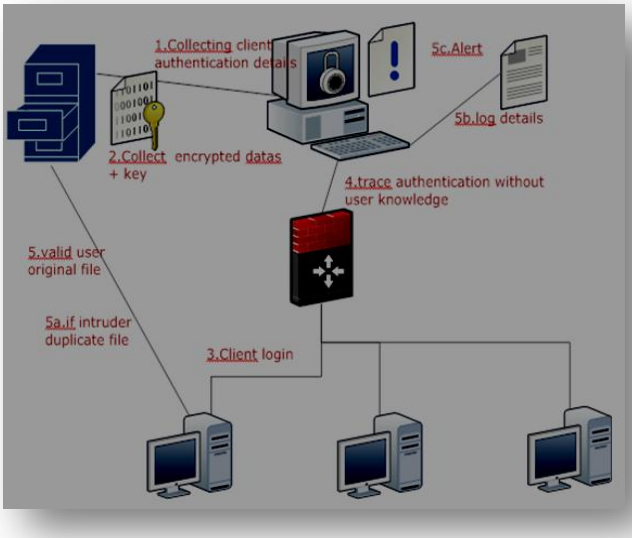

Figure 1. Proposed MIP system architecture

An intrusion detection systems methodology (IDS) is concerned with the detection of hostile actions.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 6, Issue 8, August 2016)

Moreover, this selected methodology will present two main techniques i.e. the first technique of anomaly detection in general investigates issues associated with contradiction/deviations from normal routine system/user behavior whereas the 2nd technique employs signature detection approach use to distinguish between attack or anomaly signatures and known ID signatures like MAC and IP of the client or Peer system. There are different IDS tools for exploiting IDS information such as a) host based IDS (HIDS) which exploit host details from single host b) network based IDS (NIDS) which exploit IDS information from multiple signals of a local network[2].

Our work is based on the assumption that the pair (*a, b*) uniquely identifies a machine (until rebooted), where a MAC and b IP. With *machine*, we refer to a single running system (physical or virtual), possibly behind a NAT gateway. Of course, this assumption is only valid assuming that no two machines with the same operating system (same tick scale) are booted at the same time. Even when using network or port address translation, a 4-tuple (srcaddr, srcport, destaddr, destport), containing source IP address, source port, destination IP address, and destination port uniquely identifies (one direction of) a TCP connection.MIP filtering MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. While the restriction of network access through the use of lists is straightforward, an individual person is not identified by a MAC address, rather a device only, so an authorized person will need to have a whitelist entry for each device that he or she would use to access the network. While giving a wireless network some additional protection, MAC filtering can be circumvented by scanning a valid MAC (via airodump-ng) and then spoofing one's own MAC into a validated one. Dynamic alert system and logging system is maintained.

We propose a different approach for securing data in the network using offensive decoy technology. We monitor data access in the cloud and detect abnormal data access patterns. we launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user's real data. We use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data the decoys, then, serve two purposes:

(1) Validating whether data access is authorized when abnormal information access is detected, and
(2) Confusing the attacker with bogus information.

MIP Filter Profiling

It is expected that access to a user's information in the server will exhibit a normal means of access. User profiling is a well known technique that can be applied here to model how, when, and how much a user accesses their information in the Server. Such 'normal user' behavior can be continuously checked to determine whether abnormal access to a user's information is occurring. This method of identity-based security is commonly used in fraud detection applications. Such profiles would naturally include volumetric information, how many documents are typically read and how often. These simple user specific features can serve to detect abnormal Server access based partially upon the scale and scope of data transferred [4].

Decoy System

Decoy data, such as decoy documents, honey pots and other bogus information can be generated on demand and used for detecting unauthorized access to information and to „poison" the thief's ex-filtrated information. Serving decoys will confuse an attacker into believing they have ex-filtrated useful information, when they have not. This technology may be integrated with user behavior profiling technology to secure a user's data in the Server. Whenever abnormal and unauthorized access to a server service is noticed, decoy information may be returned by the Server and delivered in such a way that it appear completely normal and legitimate. The legitimate user, who is the owner of the information, would readily identify when decoy information is being returned by the Server, and hence could alter the Server's responses through a variety of means, such as challenge questions, to inform the Server security system that it has incorrectly detected an unauthorized access. In the case where the access is correctly identified as an unauthorized access, the Server security system would deliver unbounded amounts of bogus information to the attacker, thus securing the user's true data from can be implemented [5].

IV. Conclusion

Nowadays, the rapid growth of designing and developing new techniques to secure data transferring over online environments have been deployed against certain network-oriented attacks like IP spoofing, packet storms, etc. that can be detected via IP datagram examination. This paper presents ADS, which deploy virtual agent based intrusion detection system during the attack from unknown IP, which lacks in existing IDS. The paper also presents process flow of the proposed model. The expected results presented in the paper shows the credibility of the proposed model.

REFERENCES

[1] Al-SammarraieHosam,Center for IT Multimedia, University and,SainsMalaysia,Penang,Malaysia, IEEE, Vol.06, No.1, March 2015.

[2] Shakeel Ahmad School of Mathematical sciences, University Sains Malaysia, Institute of Computing and Information Technology, Gomal University, Pakistan Penang, Malaysia,IEEE.

[3] Adli Mustafa School of Mathematical sciences, Universiti Sains Malaysia Penang, Malaysia,IEEE.

[4] Chao Gong, KamilSarac, "IP Traceback based on Packet Marking and Logging"

[5] Merza Abbas Center for IT and Multimedia, Universiti ,Sains Malaysia Penang, Malaysia in Proc. IEEE Int. Conf. Commun.(ICC).

[6] S. Knight, H. X. Nguyen, N. Falkner, R. Bowden, and M. Roughan, "The internet topology zoo," IEEE J. Sel. Areas Commun., vol. 29, no. 9, pp. 1765–1775, Oct. 2011.