International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

Anomaly Threat Detection System using User and Role-Based Profile Assessment

U. Indumathy, M. Nivedha, Mrs. K. Alice
Department of Computer Science and Engineering,
G.K.M. College of Engineering and Technology, Chennai, Tamil Nadu, India

ABSTRACT

In network security the organizations are ever-growing to identify insider threats. Those who have authorized access to sensitive organizational data are placed in a position of power that could well be abused and could cause significant damage to an organization. Traditional intrusion detection systems are neither designed nor capable of identifying those who act maliciously within an organization. We describe an automated system that is capable of detecting insider threats within an organization. We define a tree-structure profiling approach that incorporates the details of activities conducted by each user and each job role and then use this to obtain a consistent representation of features that provide a rich description of the user's behavior. Deviation can be assessed based on the amount of variance that each user exhibits across multiple attributes, compared against their peers. We have performed experimentation using that the system can identify anomalous behavior that may be indicative of a potential threat. We also show how our detection system can be combined with visual analytics tools to support further investigation by an analyst.

Keywords: *Intrusion, Cyber security, Insider threat*

I. INTRODUCTION

The insider threat problem is one that is constantly growing in magnitude, resulting in significant damage to organizations and businesses alike. Those who operate within an organization are often trusted with highly confidential information such as intellectual property, financial records, and customer accounts, in order to perform their job. If an individual should choose to abuse this trust and act maliciously toward the organization, then their position within the organization, their knowledge of the organizational systems, and their ability to access such materials means that they can pose a serious threat to the operation of the business. To avoid such problem we uses insider threat algorithm by attaching the threat program along with the message or important file then send to one client to another client

1.1 Scope of the project

Over the years, technological advancements have meant that the way organizations conduct business is constantly evolving. It is now common practice for employees to have access to large repositories of organization documents electronically stored on distributed file servers. Many organizations provide their employees with company laptops for working while on the move and use e-mail to organize and schedule appointments. Services such as video conferencing are frequently used for hosting meetings across the globe, and employees are constantly connected to the Internet, where they can obtain information on practically anything that they require for conducting their workload. Given the electronic nature of organizational records, these technological advancements could potentially make it easier for insiders to attack. Our scope of project is to reduce the insider attack by encrypting the message that we use to pass from one client to another client.

II. RELATED WORKS

The topic of insider threat has recently received much at-tention in the literature. Researchers have proposed a variety of different models that are designed to prevent or detect the presence of attacks (e.g., [3] and [4]). Similarly, there is much work that considers the psychological and behavioral character-istics of insiders who may pose a threat as means for detection (e.g., [5]–[7]). Kammüller and Probst [8] considered how orga-nizations can identify attack vectors based on policy violations, to minimize the potential of insider attacks. Likewise, Ogiela and Ogiela [9] studied how to prevent insider threats using hierarchical and threshold secret sharing. For the remainder of this section, we choose to focus particularly on studies that address the practicalities of designing and developing systems that can predict or detect the presence of insider threat.

Early work by Spitzner [10] discusses the use of honey-pots (decoy machines that may lure an attack) for detecting insider attacks. However, as security awareness increases, those choosing to commit insider attacks are finding more subtle methods to cause harm or defraud their organizations, and thus, there is a need for more sophisticated prevention and detection. Early work by Magklaras and Furnell [11] considers how to estimate the level of threat that is likely to originate from a particular insider based on certain profiles of user behavior. As they acknowledge, substantial work is still required to validate the proposed solutions. Myers *et al.* [12] considered how web server log data can be used to identify malicious insiders who look to exploit internal systems. Maloof and Stephens [13] proposed a detection tool for when insiders violate need-to-know restrictions that are in place within the organization. Okolica *et al.* [14] used probabilistic latent semantic indexing with users to determine employee interests, which are used to form social graphs that can highlight insiders. Liu *et al.* [15] proposed a multilevel framework, which is called sensitive information dissemination detection, that incorporates network-level application identification, content signature generation and detection, and covert communication detection.

III. SYSTEM ANALYSIS

A. EXISTING SYSTEM:

In the anomaly detection technique, the system defines a model for the normal behavior of the network and detects any deviation from this normal model as an anomalous behavior. Unlike the Misuse detection, an anomaly detection system with a well-defined normal model can detect new attacks, and there is no need to manually update attack signature library. With better detection performance and no need for manual updates, the anomaly detection is a promising technique, and it is actively pursued by researchers.

DISADVANTAGES :

- Security Issues
- Slow Processing
- Inaccurate

B. PROPOSED SYSTEM:

we study multi-virus spreading dynamics, where multiple viruses attempt to infect 802.11 wireless network while possibly combating against each other because, Specifically, we propose and analyze a general model (and its two special cases) of multi-virus spreading dynamics in arbitrary networks This allows us to draw various insights that can be used to guide security defense. Our technique has a good tolerance against frame loss. The main contributions of our work are the development of an efficient wireless anomaly detection system that overcomes the challenges of anomaly detection algorithms such as high false alarms, context dependency and frame losses.

ADVANTAGES OF PROPOSED SYSTEM:

1. It used to keep our message are high security and confidential.

2. Easily Identify the Attacks

C. SYSTEM ARCHITECTURE:

The architecture of the detection system is detailed in Fig. 1. Here, the detection system connects with a database that con-tains all available log records that exist for the organization. Such examples may be computer-based access logs, e-mail and web records, and physical building access (e.g., swipe card logs). All records for the current date are retrieved and parsed by the system. For each record, the user ID is used to append the activity to their daily observed profile. Likewise, the activity is also appended to the daily observed profile of their associated role, if applicable. Once the daily observation profiles are constructed, the system proceeds to assess each user

based on three levels of alerts: policy violations and previously recog-nized attacks, threshold-based anomalies, and deviation-based

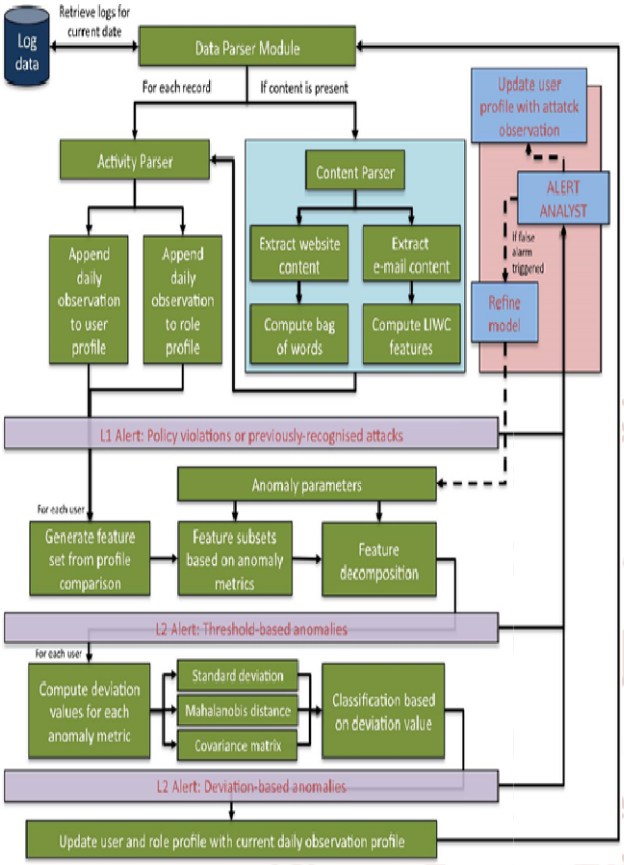


Fig .1(a)

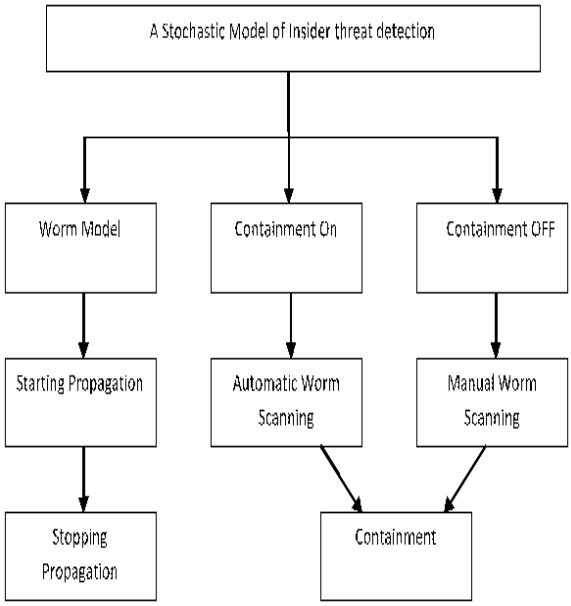


Fig .1(b)

IV. SOFTWARE DEVELOPMENT

MODULES:

- P2P NETWORK MODULE
- QUANTITIES IN MODELING
- SCANNING HOSTS AT DIFFERENT LAYERS
- MALWARE PROPAGATION

MODULE DESCRIPTION:

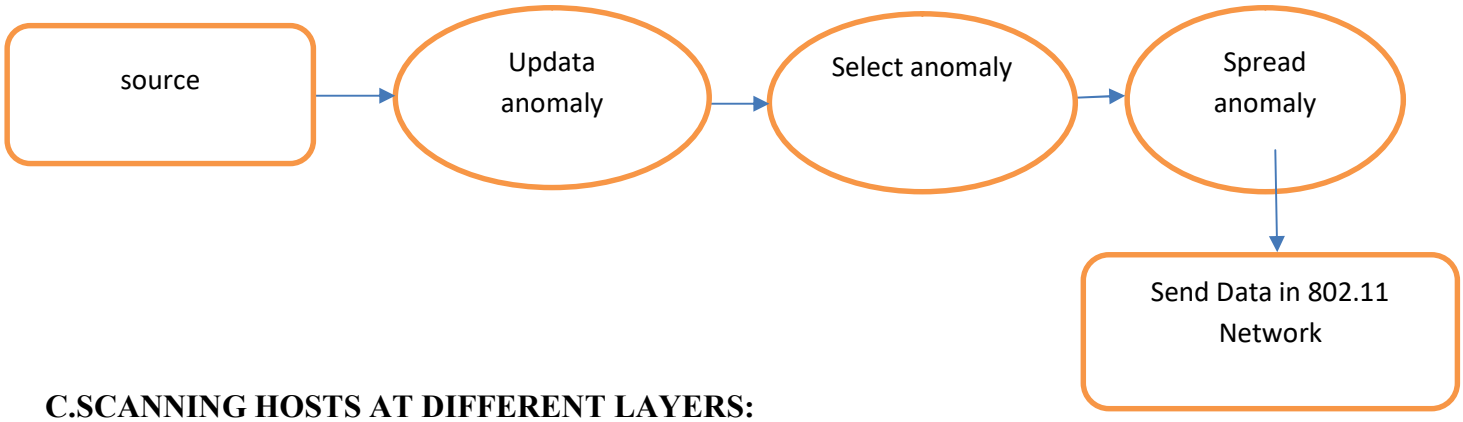
A. P2P NETWORK MODULE:

The use of peer-to-peer (P2P) networks as a vehicle to spread malware offers some important advantages over worms that spread by scanning for vulnerable hosts. This is primarily due to the methodology employed by the peers to search for content. For instance, in decentralized P2P architectures such as Gnutella where search is done by flooding the network. The design of the search technique has the following implications: first, the worms can spread much faster, since they do not have to probe for susceptible hosts and second, the rate of failed connections is less. Thus, rapid proliferation of malware can pose a serious security threat to the functioning of P2P networks.

B. QUANTITIES IN MODELING:

The malware propagation model of a worm reflects the fractions of vulnerable hosts that are infected, active, and retired over time. A scan message that does not hit any vulnerable host does not change these numbers. Thus, modeling should only be based on the event of a scan message hitting a vulnerable host. When that event happens, all aforesaid numbers change. We derive themodel by analyzing the precise amounts by which they change.

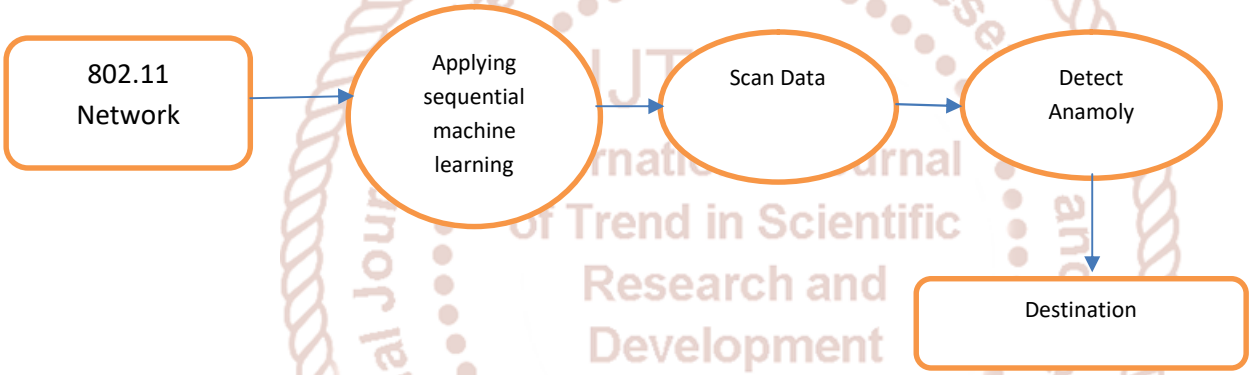
Level 1:



C.SCANNING HOSTS AT DIFFERENT LAYERS:

An active infected host never changes its layer by hitting a new infection. This is because the layer of a host indicates how many old infections the active host has hit till that time, and hitting a new infection does not change that. However, when it hits an old infection, it takes a jump, moves to the next layer, and becomes either ineffective or nascent depending on whether it jumps into a covered area or not.

Level 2:



D. MALWARE PROPAGATION:

The transfer of information in a P2P network is initiated with a search request for it. This paper assumes that the search mechanism employed is flooding, as in Gnutella networks. In this scenario, a peer searching for a file forwards a query to all its neighbors. A peer receiving the query first responds affirmatively if in possession of the file and then checks the TTL of the query. If this value is greater than zero, it forwards the query outwards to its neighbors, else, the query is discarded. In our scenario, it suffices to distinguish any file in the network as being either malware or otherwise.

V. CONCLUSION

This paper is developed based onanomaly threat detecting method and proposed to insider threat detection to reduce and control the insider attacker with used analysis the user and role based profile assessment which used reduce 100% of insider threat detection.

VI. REFERENCE

1) IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Standard 802.11-1997, 1997. [Online]. Available: http://dx.doi.org/10.1109/IEEESTD.1997.85951

2) IEEE802.11:WirelessLANs. [Online].Available:http://standards.ieee.org/about/get/802/802.11.html, accessed Nov. 21, 2011.

3) Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE Standard 802.11i-2004, Jul. 2004.

4) C. He and J. C. Mitchell, "Security analysis and improvements for IEEE 802.11i," in Proc. 12th Annu. Netw. Distrib. Syst. Security Symp. (NDSS), San Diego, CA, USA, Feb. 2005, pp. 90–110.

5) A. Sheth, C. Doerr, D. Grunwald, R. Han, and D. Sicker, "MOJO: A distributed physical layer anomaly detection system for 802.11 WLANs," in Proc. 4th Int. Conf. Mobile Syst., Appl. Services, Uppsala, Sweden, Jun. 2006, pp. 191–204.

6) Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC layer spoofing using received signal strength," in Proc. IEEE 27th Annu. Conf. Comput. Commun. (INFOCOM), Apr. 2008, pp. 13–18.

7) W. M. Suski, II, M. A. Temple, M. J. Mendenhall, and R. F. Mills, "Using spectral fingerprints to improve wireless network security," in Proc. IEEE Global Commun. Conf. (GLOBECOM), Nov./Dec. 2008, pp. 1–5.