ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

Context-Aware Intrusion Detection System in Distributed Systems

V Jasmine[1], R Santhana Lakshmi[2]

P.G. Student, Department of Computer Science and Engineering, Raja College of Engineering and Technology, Veerapanjan, TamilNadu, India[1].

Assistant Professor, Department of Computer Science and Engineering, Raja College of Engineering and Technology, Veerapanjan, Tamil Nadu, India[2].

ABSTRACT: Immunology inspired Computer Security is one of the important factor in network operation system. In Distributed Systems Intrusion Detection System is used to find the attackers and protects the system from malicious activity. Current network security technologies essentially intend to simply block threats. However this will kill the adaptability of the system and consequently jeopardising the overall system adaptability. The principle here is to propose a new threat awareness strategy to reconfigure and adapt the file access rights for the Management Information Base (MIB). MIB provides an interface between the managed devices. The threats and attacks are to be classified, filtered and controlled using K-Medoid clustering algorithm. The Algorithm classifies the data instances based on their behaviour into normal and attacks. Based on the information theoretical analysis, the coherent relationship between the adaptability, autonomy and vulnerability is broken thus maximizing adaptability and reducing the vulnerability of the system simultaneously.

KEYWORDS: Intrusion Detection System, Vulnerability Assessment, threat awareness analysis.

I. INTRODUCTION

Widespread Distributed System uses software to co-ordinate tasks and to share the resources of the system so that the users perceive as a single integrated computing facility. The Systems co-ordinate and communicate by passing messages and interact with each other in order to achieve a common goal. Some of the problems faced by distributed systems are concurrency of components and independent failure of components.

Security is one of the leading concerns in developing distributed systems. Since the integration of different components in a distributed manner the development of technologies to identify system threats is important in securing the distributed systems. A distributed System must accommodate to different heterogeneous components and also it faces threats like attacks on data integrity denial of service, hardware and software failure involving the individual components of the system.

An Intrusion detection system (IDS) is software that monitors the inbound and outbound activities of a system and identifies patterns that compromise or break into the system. IDS can be applied in different ways to detect suspicious traffic. The major classifications are Active and Passive IDS, Network Intrusion detection and Host Intrusion detection system. Active IDS are used to block threats automatically without the human intervention. A passive IDS monitors and analyze the network traffic activity and alerts the user about the potential attacks. Network intrusion detection usually consists of a network interface card that can be placed along the network segment and monitors the traffic on that segment. Host Intrusion detection system monitors the systems on which the agents are installed and are not used to monitor the entire network. Signature based Intrusion detection system maintains a database of predefined attack signatures and known system vulnerabilities. Signature refers to the recorded evidence of an intrusion or attack. The main drawback of Signature based IDS is the continuous updating and maintenance of the signature database. Behaviour based IDS references a normal system pattern to identify active intrusion attempts. Higher false alarm rate is one of the drawbacks of this system.

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

The Intrusion Detection System in the current network is not capable of identifying new attacks without knowledge or profiles. The standards used here tend to identify the attacks, prioritize and intend to block those at higher risks. However this will kill the adaptability of the system. Therefore it is not capable to cope up with the complex environment in the current network infrastructure.

The proposed work is based on a new threat awareness strategy inspired by the human immune systems. The threat awareness strategy aim to reconfigure the systems adaptability rights for the Management Information Base.MIB provides an interface between the managed devices. To analyze the security of the system, the properties like Autonomy, Adaptability and vulnerability. There is a coherent relationship between adaptability, autonomy and vulnerability.

Adaptability refers to the ability of a system to respond to unanticipated environment. Autonomy is the number of heterogeneous units to co-operate efficiently to achieve common goals. Vulnerability is the weakness which allows the attacker to reduce the assurance of information. These three factors form a basis for the proposed work. Based on the information theoretical analysis, the coherent relationship between the adaptability, autonomy and vulnerability is broken down maximizing adaptability and reducing vulnerability of the system simultaneously.Paper is organized as follows. Section II describes the network model of the intrusion detection system. The flow diagram represents the step of the algorithm is given in Section III. Section IV presents experimental results showing results of the detection system. Finally, Section V presents conclusion.

II. RELATED WORK

Previous works focuses on Misuse based detection of intrusion. Misuse relies on a set of attack signatures. The attack signatures are information that is used to identify an attacker who tries to exploit a known operating system or application vulnerability. The signatures are compared with the stream of data and attempts to verify the definite signature is occurring. Misuse based IDS are fast but not capable of detecting new attacks. Agent based IDS is used to find new attacks. The agents roam over the network to find any deviation in the incoming stream of data, if alteration founds in the traffic or the packets received the agent alerts the system about the new behaviour. The agents sometimes fail to detect the traffic and also alert the system by false alarms when there are no significant changes in the traffic.

In [4] the distributed agent architecture for Intrusion, the IDS is based on the anomaly approach using statistical methods. These systems have the advantage of being able to detect unknown attacks, but they suffer from the difficulty of high number of alarms caused by unusual activities. These IDS are not capable of detecting attack scenarios over an extended period of time. One of the major problems here is not all the abrupt changes are anomalies, so it is difficult to determine the right threshold above which the anomaly is to be considered as intrusion.

Based on Octopus IIDS [3] the intrusion detection system is classified into two layers as classifier and anomaly detector. The classifier is responsible for collecting network traffic. Anomaly detector is classified into four categories U2R, DoS, probe and R2L.This detector gets input from the support vector machine which receives traffic from the classifier. The IDS generally focus on the attack types already defined and not able to detect the new anomalies happening in the environment.

The flooding attacks are identified by the covariance matrix modelling technique. The abnormal packets are amassed quickly in order to capture the resources. The statistical properties within a time period reflect the traffic behavioural properties of the flooding attacks, which is different from that of the normal traffic. Therefore, the statistical properties contained in the temporary sequential samples can be used to detect the flooding attacks. To exhibit the correlativity of the underlying network traffic, statistical covariance matrices to model the sample sequences of equal and fixed length is considered. Each element in a covariance matrix describes the correlation between any two monitored features of the corresponding sample sequence.The modelling process utilizes the correlations among network features provided by the passive-network-monitoring devices.

In Intrusion Detection using K-Medoid clustering [8], the data instances are grouped based on their behaviours. The resulting clusters are then classified into normal and attacks using SVM classifiers. Instead of taking the mean value of the cluster of data instances, the most centrally located object is considered as the reference point and the instances are grouped to the centroid or the medoid. This partitioning based on the distance metrics helps to classify the data instances and identify the data which is malicious in the network.

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

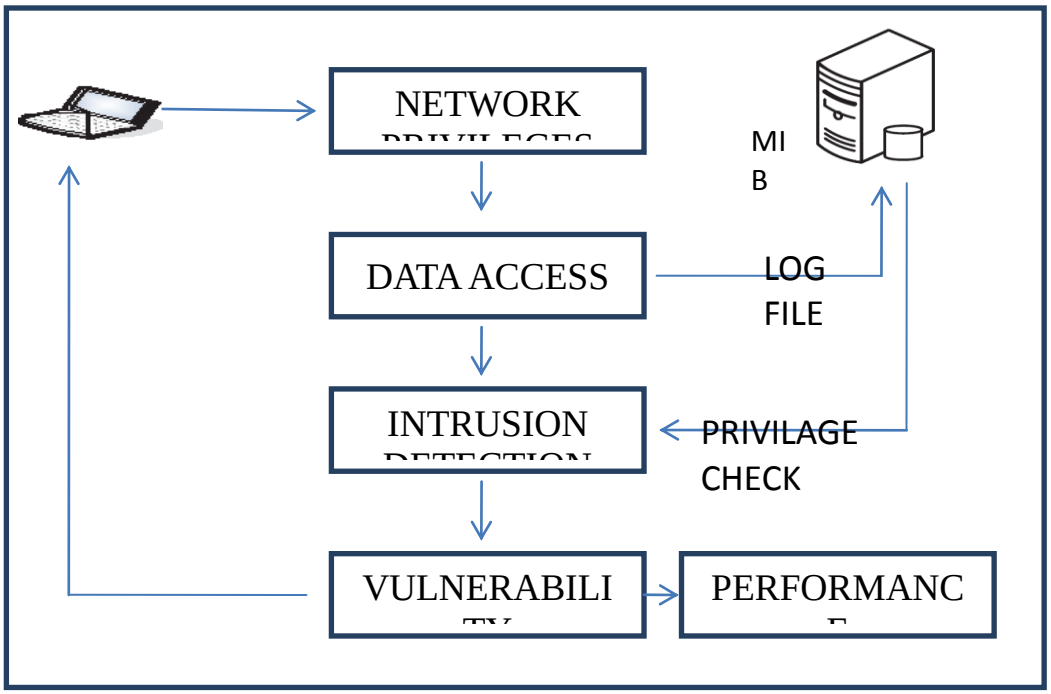
Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

III. NETWORK MODEL

An open system access for allowing threats, the network is the primary constraint in the distributed system. The System files and call logs are maintained individually for every system in a database called the Management Information Base (MIB). MIB provides naming service to all the managed devices. By maintaining this naming of the devices MIB monitors the requested information. Initially all files in the system connected in the network are readable and some files are writable. However the writable information can alter the process of the file access rights. Making the system more vulnerable depends on the information content in the system. When there is more number of writable information content the system is subjected to more modifications and in turn is vulnerable. If any system tries to access the files in the system then it is recorded and maintained in the MIB database. The database is updated so that the security of the information can be modified based on the time and also the incoming data. In the analysis of system security factors like reliability, robustness, adaptability, and autonomy are considered. The definitions are as follows.

Reliability of a system is the ability of a system to continue functioning when faults happen.
Robustness is the capability of a system to recover from failure.
Rewritability (RW) of the system's information can be calculated by the number of readable information to that of the writable information security.

The work focuses on the measurement of system vulnerability by the system status and making decisions to maximize the adaptability of the system thus reducing the vulnerability of the system.This illustrates the following network architecture diagram.
In this architecture, network is created and file access privilege for each file in the system of the network is assigned individually. The access privilege of the system varies on a time basis. All privileges are recorded in the Management Information Base (MIB) database. Whenever a system is trying to access the files in the network system, it is recorded in the MIB log file. Using these log files, this system analyses the intruder for accessing data or try to change the privelages in the network.



ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

Based on the Intruder detection system, performance is calculated in the factors of vulnerability, anomaly and adaptability. Writablility and adaptability of a system is similar to the system vulnerability. The data instances are classified filtered and the critical information is found out with the help of K-medoid Clustering algorithm. With the analysis of system vulnerability, the system can detect system status for critical processes and take actions to maximize system adaptability. To implement vulnerability the following formula can be calculated.

$$V(sys) = (W_{xi})/(1+R_{xi}) \quad ....(1)$$

Where $W_{xi}$is calculated from

$$W_{xi} = TN_{Wi}/ (1+TN_{Ri})...(2)$$

MIB provides interfaces that monitoring network status and maintain the requested information from any system that has the tree structure.

IV. ALGORITHM IMPLEMENTATION

The MIB Status is updated in a predefined update time. This will helps us to reconfigure the priviledge access to the system information.

MIB Information Flow-Pseudo code

1. **If** predefined update time reaches **then**
For all MIB information in an instance k **Do**
2. Find relevant information that are required
3. Configure MIB variables.
4. **End For**
5. **For** all MIB Information at an instance k **Do**
6. Apply Constraints ←internal misconfiguration errors, disruptive influences and system vulnerability conditions.
7. call the function update InfoFlow()
8. **End For**
9. **End If**

To analyze vulnerability in the system, k-medoid clustering algorithm is implemented. In this Algorithm the data instances are grouped based on their behaviour as normal and attacks. After clustering of data instances a representative of the cluster is determined .The representative of the cluster is named as the medoid and the remaining objects are clustered with the medoid.

`

Algorithm: Vulnerability detection

1. Create cluster in the network
2. Based on the privilege info in MIB
    a. Impleents the cluster head
    b. C.H records privilege info.
3. For each node
    a. If C.H.info < MIB.info
        i. Calculate min_distance
    b. Else
        i. Store C.H info to MIB
4. Repeat
5. Evaluate min distance of each cluster for V(sys)

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

6. Analyze V(sys)

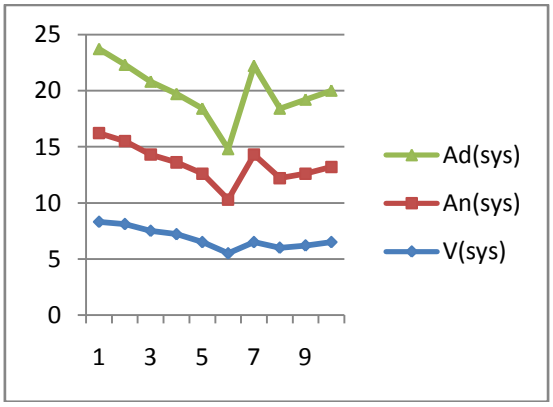
Instead of taking the mean value of nodes in a cluster, the most centrally located nodes have collect information from other nodes in the network and analyse the privileges of each node form MIB.

V. EXPERIMENTAL RESULTS

To analyze vulnerability in the network, our experiment is based on both simulation and model based approach. This system mainly focuses the system's activities based on file access privileges and storing privilege information in a separate network database called MIB. This can be analysed in the following categories 1. The file access changes. 2. Writable privilege variations, 3. Multiple nodes access same file with different privileges, 4. Observed internal errors when applicable.

File attributes are converted to appropriate types of values and that are normalized. Samples with unknown threats are treated as attacks. Then it can be categorizedto {0,1} where 0 represents the normal class and 1 represents the abnormal class. These categories are treated differently for the use in k-mediod clustering and it separates the data type.

From the dataset collected from MIB, that is limited and containing 1000 records. Each record is extracted by implementing the intrusion detection system of vulnerability analysis, different performance measures evaluated. The graph is plotted from vulnerability threshold value with more number of nodes.



In the graph, vulnerability increases initially and decreases in a constant movement. In the same time adaptability and anomaly are increased in a constant movement. That is if vulnerability decreases then adaptability increases. Therefore threats are sometimes vulnerable and that are stopped immediately to reduce vulnerability.

VI. CONCLUSION

The paper describes the relationship between the adaptability, autonomy and vulnerability. In reality the uncertainty of the systems makes it difficult to get a solution for these problems. The multiple layered threat awareness system helps us to assess the risks and vulnerabilities posed by the attackers in the network. The updating of MIB variables helps to change the privilege access over a period of time.

Current System Vulnerability is used to detect how much the system is affected and to improve the adaptability of the system. The coherent relationship between the adaptability, autonomy and vulnerability is broken and the system adaptability is raised. The self adaptable scheme enables the reduction of vulnerability in the distributed systems.

REFERENCES

[1] Frank Jiang, Daoyi dang,"Agent Based Self Adaptable Context Aware Network Vulnerability Assessment.", IEEE Transactions on network and service management, September 2013.

ISSN (Online): 2319-8753
ISSN(Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 4, Special Issue 5, April 2015*

International Conference On Emerging Trends in Engineering and Technology (ICETET'15)

On 13th & 14th March 2015

Organized by

Pandian Saraswathi Yadav Engineering College, Arasanoor, Sivagangai, Tamilnadu, India

[2] Cohen.I and Segel. L, "Design Principles for the Immune Systems and Other Distributed Autonomous Systems". Santa Fe Institute Studies in theSciences of Complexity, Oxford University Press, 2001.
[3] Emran. A , ye. S et al., "Multivariate statistical analysis of audit trails for host-based intrusion detection," IEEE Trans. Computers, vol. 51, no. 7, pp. 810–820, 2002.
[4] Farah Barika, Nabil El Kadhi, "Distributed agent architecture for intrusion detection based on new metrics", IEEE Trans evolutionary Computation, 2009.
[5] Fung C.J, Zhang. J, and Boutaba. R, "Effective acquaintance management based on Bayesian learning for distributed intrusion detection networks," IEEE Trans. Network and Service Management, vol. 9, no. 3, pp. 320–332, 2012
[6] Kumar.G and M. Sachdeva, "The use of artificial intelligence based techniques for intrusion detection: a review," Artificial Intelligence Rev., vol. 34, pp. 369–387, 2010.
[7] Paulo M. Mafra Vinicius Moll, Joni da Silva "Octopus-IIDS: An Anomaly Based Intelligent Intrusion Detection System",IEEE Trans 2011.
[8] Roshan Chitrakar ,Huang "Anomaly Detection using Support Vector Machine Classification with k-Medoids Clustering" IEEE Transactions, 2012.
[9] Lahmadi. A and Festor. O, "A framework for automated exploit prevention from known vulnerabilities in voice over IP services," IEEE Trans 2011.
[10] Lee.W.K, S. J. Stolfo, and K. W. Mok, "Adaptive intrusion detection : a data mining approach" Artificial Intelligence rev, vol 14,2000.