International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-1 Issue-2, July 2012

Layered Approach of Intrusion Detection System with Efficient Alert Aggregation for Heterogeneous Networks

Lohith Raj S N, Shanthi M B, Jitendranath Mungara

Abstract: ***Protecting data from the intruders on internet or on the host systems is a very tedious task. The Intrusion Detection System is a technology for detecting suspicious actions or malicious behavior in a system from the unauthorized users or so called intruders. Alerts are produced during the intrusion activity, but when more number of alerts is produced then handling of these alerts becomes difficult on IDS. In this paper, we propose a layered approach for IDS where the alert information is represented dynamically in the form of layers and we propose an alert aggregation algorithm where an attack instance is created for similar type of alerts produced and this is clustered to form a meta-alert which can reduce the number of alerts produced without losing any information. This technique has approaches like generative modeling, in this case the beginning as well as the completion of attack properties and details can be detected and it is a data stream approach, where duplicate or the alerts which are observed many number of times are processed only a few times. By applying these techniques and alert aggregation we can reduce the number of false alert rate and number of alerts.***

The goal of the project is to generate meta-alerts from the proposed alert aggregation algorithm and represent all the alert information or the intruder activity on a dynamically representing model. The alert produced and the details of the alert and the action taken are represented in the form of layers on a distinctive layered model. The details of the alert are represented using these layers and further to form a meta-alert. Meta-alerts contain all the relevant information but the amount of data can be reduced progressively. Using the data sets, it is possible to reduce the number of alerts produced while number of missing meta-alerts is extremely low and represent all the alert information in the form of layers on a model.

Keywords: Network Security, Intrusion Detection, Alert Aggregation, Data-Stream Approach.

I. INTRODUCTION

An Intrusion detection system (IDS) is a system which monitors network or system activities for intrusion activities like malicious activities and other threats to the system by producing an alert or by reporting to the management station. Some systems like Virtual Private Network (VPN) systems and mechanisms like authentication mechanisms or encryption techniques play a very important role to provide security for the system and guarantee data security. They are primarily focused on identifying problems with security policies, documenting existing threats and deferring the threats from violating security policies. These systems provide security for network systems as well as the host systems against different threats and this will typically record information related to observed alerts and notify security administrators and produce reports.

The existing IDS which are present are quite reliable in producing the alert but when more number of alerts is produced it degrades the system performance and handling of the alert information becomes very difficult for the system admin. The misuse and anomaly detections which are the detections made by IDS uses Snort or Simple Vector Machines or any other method to detect the intrusion activity on the network or the host systems. The IDS are basically classified as Network Based Intrusion Detection System (NIDS) and Host Based Intrusion Detection System (HIDS) where both act as the detection system from the intruders. Network based IDS are basically used in the network related system where NIDS is basically made for monitoring network traffic. It responds very quickly during unsuccessful attacks or problems in network real time. Host based IDS is IDS which is installed on the host systems where it acts as encryption device for the intruders and unambiguous activities. The existing Intrusion Detection System is very challenging for the security administrators to inspect large numbers of alerts produced and to take action where many alert produced might be false with high probability.

In the proposed system the IDS is represented in the form of layers, so that the system admin can keep a track of information of the intruder to take further action. Using VPN the admin can give the privileges to the user like user level, process level and the packet level privileges. The proposed alert aggregation algorithm generates the meta-alert by grouping the attack instances which are generated by different alerts. By using the proposed alert aggregation technique we can reduce the number of false alert rate which are generated by the same attack type with different targets systems. By implementing the data stream modeling we can make the system foolproof and efficient in generating the alerts. By using all these techniques the goal of reducing the amount of alerts can be achieved without losing any important information.

Revised Manuscript Received on 30 July 2012
*****Correspondence Author(s)
Lohith Raj S N*, M.Tech, Department of Computer Science and Engineering, CMRIT, Bangalore, India.
Mrs. Shanthi M B, Assistant Professor, Department of CSE, CMRIT, Bangalore, India
Dr. Jitendra Nath Mungara, Professor and Dean, Department of CSE and ISE, CMRIT, Bangalore, India.

II. REVIEW OF LITERATURE

Networks are protected from intruders using many firewalls and some encryption techniques and out of them many are not sufficient and very effective. Most IDS present on ad hoc networks for mobile are focusing on either routing protocols or the efficiency of the routing protocols on ad hoc but this does not satisfy or it fails to solve the security issues and act on attacks like DOS (Denial of Service) or other malicious information. The goal is to provide security for wireless networks by providing security like availability, confidentiality, integrity, authentication, and anonymity, to mobile users. The paper "Agent Based Efficient Anomaly IDS in Adhoc networks"[2] provides security agents and data mining approaches to prevent anomaly intrusion prevention in Adhoc networks for mobile. The neighboring nodes are monitored by mobile agents and these obtain the information to determine the repeated anomalous types before data is sent. Now this system was successful in reducing the false alarm positives and was able to prevent the attacks in an Adhoc networks.

Wireless Sensor Network (WSN) provides effective intrusion detection strategy in many applications. In the application which consists of WSN was effective in detecting an intruder in the network based systems, the intrusion activity like incorrect, anomalous or inappropriate moving attackers are basically detected using WSN which are considered to be effective in detecting intrusion activity in Wireless networks. The WSN are run on parameters like sensing range and node density which is the fundamental issue in detection probability. In the paper "Intrusion and Detection of Homogenous and Heterogeneous Wireless Sensor Networks" [3], considered for two WSN models i.e., heterogeneous and homogeneous WSN. Two sensing models are considered for the detection probability they are multiple-sensing and single-sensing detection. The related conditions for detection probability in WSN like broadcast reach ability and network connectivity, which ensure the detection probability in WSN.

The existing IDS are efficient in detecting different attacks with high accuracy. But, they still have many disadvantages which has already provided in a number of publications and progressively work has been done to analyze IDS in order to direct further future research [5]. The presented correlation approach is reconstruction of the thread for each attack, by which for this reconstruction strategy can be seen as attack instance recognition. There is no clustering algorithm for grouping of these alerts, but arrangement of these alerts is based on the source, destination, and attack type. In [7], alerts that share the same details of source and destination address as well as source and destination port are used to eliminate duplicates. Alerts are aggregated into pre-defined groups or clusters in order to provide a more compressed view of the current situation. In [9], alert clustering is used to group alerts that belong to the same attack occurrence. Basically with all these information the process of grouping alerts i.e., alert aggregation and representing that in the form of layers are achieved and future research of representing the alert information into meta alerts and sending these information to the mobile can be achieved and the actions on the alerts can be taken by the admin instantaneously.

III. LAYERED INTRUSION DETECTION SYSTEM ARCHITECTURE

The intrusion detection agent architecture consists of the following phases grouping Intrusion Detection Agents, Intrusion Detection and Alert Generation, Alert Format and Aggregation, Intrusion Prevention and Data Stream Alert Aggregation, Log File and Mobile Alert**.**

A. Intrusion Detection Agents

Intrusion Detection Agents acts as the agents for detection of suspicious actions from the intruder activity over the heterogeneous networks on a Distributed Intrusion Detection System. The agents are classified as User Level Agent, Packet Level Agent, and Process Level Agent each performing the activities at different levels. The sensor layer acts as the layer to get the details of network systems as well as the host systems where the agent resides. The sensors in the sensor layer get all the details i.e., raw data from both network system as well as the host system. The information contains potentially valuable information which is needed to perform further processing activities. The information include the details of the host system name and the registered OS system, similarly for the network systems where it check for which network it is connected to, basically it checks with TCP/IP connections, UDP connections and gets the details of the network system connected with the Intrusion Detection System.

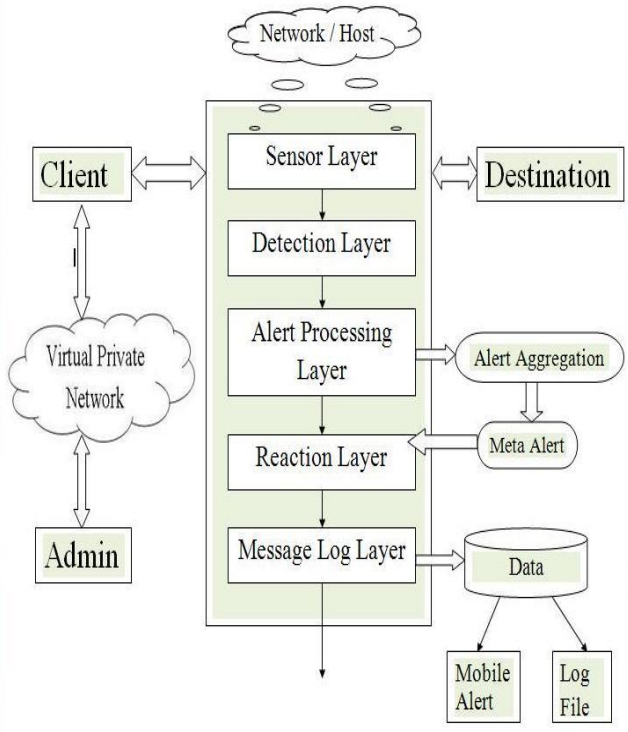

Figure 1: Layered Intrusion Detection System Architecture

Sensor Layer acts as the Sensors to get the details from host systems as well as the network systems. These raw data are sent for further processing to the detection layer. In the detection layer, the raw data are obtained as events. Detection layer acts as the protector from the intrusion activity by detecting what type of attack is going on using the detectors.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

These detectors using the data will search for any known suspicious behavior (anomaly detection), attack signatures (misuse detection) and other malicious activities. In the case of any suspicious activity or any intrusion activity, the detection layer produces alerts and forwards the details to the alert processing layers for further processing of these events. The alerts which are produced in the detection layer can be produced by installing FW in the detection layer. And the details are forwarded to alert processing layer for further processing.

The Firewall software which is installed on a system is one of the systems which generate an alert during an intrusion activity.

B. Intrusion Detection and Alert Generation

The alert generated contains the information of the alert object aggregated and on their format. The attribute values are obtained from the data produced by the sensors which is used as the input for detectors and for alert aggregation. The details obtained from the sensors in the Sensor layer and the Detection layers are the attributes of the alert produced which are independent for each and every attack instance which are used for classification in Alert Processing layer. The Attack instances are distinguished between different attack types and the alerts produced based on the attributes obtained. These Attributes obtained are, might be dependent on the attack instance used in an alert aggregation process. To identify the attacker, the attributes which represent the information like source IP address and the destination IP address and the information destination port address which is 80 for the web based attacks are dependent on the alert information produced.

C. Alert Format and Aggregation

Meta-Alerts are the result of the Alert Aggregation in the Alert Processing Layer. Alert are produced for a particular type of attack, when there is same type of attack in different instance of time then these same type of alert for a attack type is grouped together and an attack instance is formed. Similarly for different attack type where different alerts are produced will be grouped based on the attack instance at different instance of time. There is no particular clustering algorithm used for this process. The alert aggregation is a concept which is obtained from offline alert aggregation and online alert aggregation algorithm which was defined for group several attack instances belonging to various attack types. Attack instances are the formation of various attribute values which are obtained by different alerts produced. When there is grouping of similar type of alert type to form a attack instance, then these attack instances contains all the information of the attacker and the attributes by which with all these information, a meta alert can be generated. Meta-Alert is the alert which contains all the information of the attack instance by which the amount of alert can be reduced and the burden of data mining on these alerts by the security administrator can be reduced. The amount of data can be reduced substantially without losing important information. The false alerts which are produced during repeated intrusion activity of the same alert type is potentially problematic situations which can be reduced by accepting the false alerts only to certain extent.

Intrusion Detection Message Exchange Format (IDMEF) is the concept used to encode alerts produced due to intrusion activity and IDMEF is the default format. The alerts generated are changed into IDMEF format to get the attribute value for the alerts. The basic attributes present in the alert are source, node, and IP address of destination, user, and network service. Similar alert types are grouped together and the process continues to form a meta-alert. Irrelevant and the inappropriate or false alerts are considered separately and are ignored.

The basic IDMEF alert is as shown in the following format

< idmef: IDMEF –Message Version=”0.1”>
< idmef: Alert messageid=”15000”impact=” unknown”>
<idmef: Create Time ntpstamp=”0xef449129”/>
< idmef: Source>< idmef: Node>
< idmef: Address> 192.162.1.1< idmef: /address>
< idmef: /Node>< idmef: /Source>
< idmef: Target>< idmef: Node>
< idmef: Address> 172.16.25.99 < idmef: /address>
< idmef: /Node>< idmef: /Target>
< idmef: /Alert> < idmef: /IDMEF>

The process is meta-alert is carried out by merging the IDMEF format alerts and other relevant alerts to result in formation of meta-alert which is hierarchical. Meta alert is represented as root node and merged alert are considered as leaf node. When alert is generated then the new alert is compared with Meta alert and it is formed with associated group.

Proposed Alert Aggregation Algorithm

Input: Data obtained from Alert Processing Layer of n Users (U1, U2, U3…..Un)
Output: Meta-Alert m.
Method:
(1) Initialize meta list with U1
(2) Initialize meta-alert count m to 1 and i to 2
(3) Repeat
(4) Compare Ui with (Ui-1)……U1
If pattern matches
Append Ui to meta-list
Otherwise
List (m+1) ← {Ui}
Increment meta-alert count, m
(5) Increment i
(6) Until Un
(7) Return m

The meta-alerts are formed when similar type of cluster or group of alerts with same alert type is fused together. If the alert type is different based on the attack instance then it is stored onto different list and later formed with different meta-alert. When same and duplicate alert generated which has same source node and has different target nodes then these alerts are stored into different list and later ignored. To achieve this task we proposed the above algorithm.

This meta-alert aggregation algorithm has both hierarchical and incremental techniques. A single object of data is taken as a meta-data from the data set and it starts comparing with the other objects. This processing activity repeats until all of the data set has completed processing. Processing of the data is comparatively faster and the Processing time as well as the results will be based on the dataset used.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

D. Intrusion Prevention and Data Stream Alert Aggregation.

Alert aggregation for further processing of the alert uses two important concepts i.e., Data Stream modeling and generative modeling approach. Where Data Stream Modeling is an approach where similar or same alert produced is processed only a minimum number of times. The alerts which have the same source and different targets are grouped together to form a list of alerts and later ignored or rejected. The proposed intrusion detection agent is a situation aware. This is a case where it has to distinguish whether the alert produced is similar to the previous one that is done using data stream approach. Data Stream Alert Aggregation is the cluster which is formed due to data stream approach. A mixing coefficient is either zero or the reciprocal of the number of active components. With appropriate novelty and obsoleteness detection mechanisms aim at detecting these points in time with both sufficient certainty and timeliness. In generative modeling approach, the starting and the ending point of the attack instances can be detected.

E. Log File and Mobile Alert

All the alert information is represented in the layers where each layer represents with their particular action. All these information which contains all the required information about alert is represented in the message log layer. Where these message log layer information is further grouped together and can be stored on to a log file. The log file gives the information of the alerts to take further actions by the administrator. The admin can later provide the privileges for the real user.

This information can be sent to the admin when he's offline as a mobile alert. The mobile alert has all the basic information about the alert and what action is taken on the alert. Mobile acts as a great interface in getting the information of the intruder in a short message. Data mining can be applied on the attack instances if there are more number data is present on the log file. The meta-alert will incrementally updated when every time a new alert is added to the component. Meta-alerts are used from starting of the attack instance and till the attack instance is killed or till the action is taken by the administrator. The alert which are produced are grouped together to form an instance where each attack instance starting point and the completion of the attack instance is grouped together to form an attribute where this attribute forms a major role in getting the experimental results.

IV. EXPERIMENTAL RESULTS AND PERFORMANCE OF INTRUSION ALERT AGGREGATION

The performance is measured based on the alert aggregation by evaluating the details obtained which is Percentage of Detected Instances. The performance of Alert Aggregation is measured for the meta-alert where for each attack instance which is being detected is measured if there is at least one meta-alert that contains alerts of that particular alert instance. If the number of instances detected is divided with by total number of instance in data set then this data obtained in percentage gives the Percentage of Detected attack instances. The instances which are obtained by the detection layer and alert processing layer are determined to measure the percentage of detected attack instances.

The execution results consists of mainly 5 modules, which consists of Server, Client, VPN Server, Destination, DARPA Dataset. The execution of Server gives an effective representation of the layers which are represented on this probabilistic model which consists of Sensor Layer, Reaction Layer, Detection Layer, Alert Processing Layer, and the Reporting or Message Log Layer. These layers provide the effective representation of intruder information dynamically. These details can be either stored onto log file or can be sent as an alert to the mobile to which the option has been given.

The performance of alert aggregation technique has been done in three phases. In the first phase, we deal with the alerts that are generated. In the second phase, using data stream modeling repetition of alerts is avoided by grouping the alerts of same type. In the third phase, we deal with the original cause i.e., making the IDS situation aware for the alert produced and reduce then number. The processing of all these three phases are carried out and it further monitors for malicious activities and finally reports it. When a new alert is generated, it starts comparing the existing alert for any similarity measures and then it will start merging it. If the alert is found not matching then it is further set in the queue for future processing of alerts. These merging of alerts can be resulted in creating a Meta-alert. The merging of alerts are carried out by the alerts of same type can be recognized by alerts generated from same source again different targets.

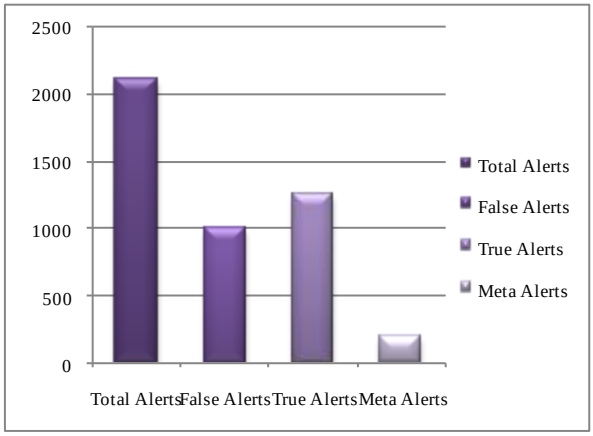

Figure 2. Meta Alert Evaluation

The performance analysis is carried out the clustering algorithm y-means algorithm where there are many clustering algorithms which are used in various applications but y-means algorithm is more versatile than other clustering algorithms, so decided to compare with y-means algorithm. The comparison of the cluster of alerts produced between different data is carried out using y means algorithm and the proposed algorithm and found that proposed algorithm shows better results compared to y-means algorithm.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

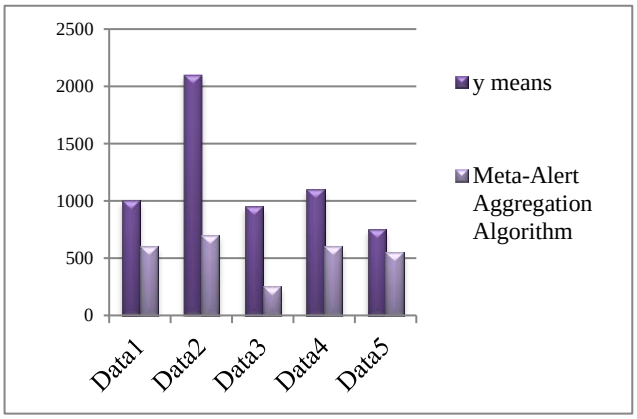

Figure 3.Performance Analysis Graph

V. CONCLUSION

The proposed algorithm to cluster the alerts to form meta-alerts and the use data stream approach and generative modeling proved that the amount of alerts can be reduced without losing any important information. The layered approach of the IDS developed, provided real time access of the alert generated and based on the alert information the actions is taken by the IDS on the intruders. The Proposed algorithm speeds up in creating the cluster of alerts i.e., meta-alerts which improves the performance of the system without losing any resource. The Proposed IDS is considered to be situation aware and more foolproof. The false alerts which are produced can be substantially reduced by using Data Stream Modeling where this is proved by getting the experimental results. The testing conducted on three different data sets showed that intruder information can be obtained without losing any information where even firewalls can be used as alert producers. In all of the cases, the amount of data could be reduced substantially without losing any important information. The representation of alert information in the form of layers provided a real time approach to act on the alerts which are produced during an intrusion activity. The intruder details can be further stored onto log file and can apply data mining to filter the data. Admin can receive a message which contains the intruder information on the mobile. The privilege is given to the client if he is considered as the true and real time user.

VI. FUTURE WORK

In this proposed system, the Mobile alert for the user or Admin is limited to small distance of communication. In future this can be extended to large wireless distributed networks. The meta-alerts which are stored onto log file can be divided based on attack instance and we can apply data mining to get a particular attack instance details. Packet level alert agent is limited to download or upload small amount of data, in future this can be extended to large amount of data. The Virtual Private Network which is used for sharing important information online can be extended to provide privileges based on the data sets, by the Admin.

REFERENCES

1. Alexander Hofmann, Bernhard Sick "Online Intrusion alert aggregation with generative Data Modeling" IEEE transactions on dependable and secure computing, VOL.8, No.2 March- April 2011
2. Agent Based Efficient Anomaly Intrusion Detection System in Adhoc networks. R. Nakkeeran, T. Aruldoss Albert and R.Ezumalai.
3. Intrusion and Detection of Homogenous and Heterogeneous Wireless Sensor Networks. Yun Wang, Student Member, IEEE, Xiaodong Wang, Member, IEEE.
4. S. Axelsson, "Intrusion detection systems: A survey and taxonomy," Chalmers University of Technology, Department of Computer Engineering, Tech. Rep. 99-15, 2000.
5. M. R. Endsley, "Theoretical underpinnings of situation awareness: A critical review," in Situation Awareness Analysis and Measurement, M. R. Endsley and D. J. Garland, Eds. Mahwah, NJ: Lawrence Erlbaum Associates, 2000, ch. 1, pp. 3–32.
6. C. M. Bishop, Pattern Recognition and Machine Learning. New York, NY: Springer, 2006.
7. M. R. Henzinger, P. Raghavan, and S. Rajagopalan, Computing on data streams. Boston, MA: American Mathematical Society, 1999.
8. A. Allen, "Intrusion detection systems: Perspective," Gartner Inc., London, UK, Tech. Rep. DPRO-95367, 2003.
9. F. Valeur, G. Vigna, C. Kr¨ ugel, and R. A. Kemmerer, "A comprehensive approach to intrusion detection alert correlation," in IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 3, 2004, pp. 146–169.
10. H. Debar and A. Wespi, "Aggregation and correlation of intrusion-detection alerts," in Recent Advances in Intrusion Detection, ser. LNCS, W. Lee, L. Me, and A. Wespi, Eds., vol. 2212. Berlin, Germany: Springer, 2001, pp. 85–103.
11. D. Li, Z. Li, and J. Ma, "Processing intrusion detection alerts in large-scale network," in International Symposium on Electronic Commerce and Security.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)