© 2017 IJSRSET | Volume 3 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Layered Approach for Intrusion Detection System Using Hidden Conditional Random Fields

M. Mangaleswaran
Assistant Professor, Department of Computer Science and Engineering, Jansons Institute of Technology, Coimbatore, Tamil Nadu, India

ABSTRACT

Intrusion detection is a vital approach to guarantee the security of computers and networks. In this paper, a new intrusion detection framework is proposed in view of Hidden Conditional Random Fields. With a specific end goal to enhance the execution of HCRFs, we present the Two-organize Feature Selection strategy, which contains Manual Feature Selection technique and Backward Feature Elimination Wrapper technique. The BFEW is a perspective determination strategy which is presented in light of wrapper approach. Experimental results on KDD99 dataset demonstrate that the proposed IDS not just have an extraordinary favourable position in identification effectiveness additionally have a higher exactness. In this paper we built up a handy test suite for showing signs of improvement the ability and accuracy of an interruption discovery framework utilize the layered CRFs. We set up changed sorts of checks at a few levels in each layer .Our structure look at different quality at each layer with a specific end goal to successfully group any encroach of security. Once the assault is identified, it is hinted through cell phone to the framework manager for protection the server framework. We set up tentatively that the layered CRFs can in this way be more expert in identifying interruptions.

Keywords : Intrusion detection system; Hidden conditional Random Fields; Conditional random fields; Anomalous Activity; Layer-based Intrusion Detection System.

I. INTRODUCTION

The rise and improvement of the system has adjusted the life of human. Lamentably, we need to handle an assortment of dangers of system interruption while getting a charge out of the straightforwardness brought by the system. Keeping in mind the end goal to shrivel and avoid the dangers, a progression of interruption anticipation strategies like firewalls have been displayed. The IDS [1] screens the occasions occurring in a framework enthusiastically, and chooses whether these activities are interruptions or recently standard practices. IDSs can be named inconsistency based or signature based by the assault discovery strategy. Another strategy for interruption discovery is to make utilization of both the typical and the anomalous conduct for preparing IDS. This joins the upsides of both the irregularity based and the mark based strategies [2]. Intrusion Detection Systems depend on two ideas; coordinating of the once in the past observed and thus known strange examples from an interior database of marks or building profiles in view of typical information and distinguishing deviations from the normal conduct [3]. In light of the sort of organization, the Intrusion Detection Systems are arranging as Network based and Host based. Organize based frameworks make an evaluation by Analyzing the system logs and parcel headers from the internal and active bundles. It has based frameworks screen's individual frameworks and utilizations framework logs extensively to settle on any choice. Interruption Detection Systems are additionally Signature based or Behaviour based. The fundamental motivation behind interruption identification is that finding the assault which is exact in the marks and additionally finding the new or imperceptible assaults proficiently and furthermore think of extensive measure of system traffics [4]. Organize Intrusion Detection Systems are set at a considered point or indicates inside the system screen movement to and starting all gadgets on the system. In a perfect world one would examine all inbound and outbound activity. HIDS Host Intrusion Detection Systems are keeping running on individual

hosts or gadgets on the system. A HIDS screens the inbound and outbound parcels from the gadget just and resolve mindful the client or chairman if suspicious action is recognized. It will investigate arrange activity and framework particular settings for adequately choice the assaults make due in the present system condition. A mark construct IDS will screen bundles in light of the system and think about them against a database of marks or examples of known noxious dangers.

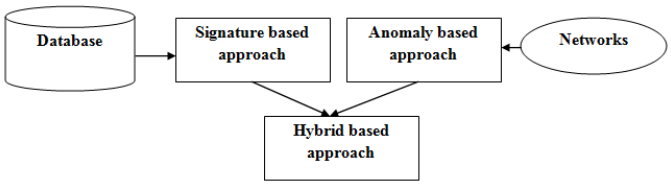

Figure 1. Generic representation of system

An IDS which is inconsistency based will screen arrange activity and look at it against a built up standard. The Generic portrayal of this framework is appeared in Fig.1. Interruption Detection Systems alludes to a program used to recognize an interruption once it happens and to keep a framework from being traded off [5]. An interruption location framework screens the exercises of a given domain and distinguishes mistaken and Inappropriate and strange movement as characterized by the Sysadmin, Audit, Networking, and Security foundation. Hybrid approach is another strategy for interruption discovery which is prepared with both the normal and the perceived abnormal examples. Mixture frameworks are proficient and perform arrangement on test information.

II. CONDITIONAL RANDOM FIELDS

Conditional random fields are a gathering of numerical displaying mode frequently connected in example acknowledgment and machine realizing, where they are utilized for organized forecast. While a basic classifier foresee a mark for a solitary specimen without respect to "neighbouring" examples, a CRF can consider; e.g., the straight chain CRF well known in acknowledged dialect handling predicts groupings of names for arrangements of information tests. CRFs are a class of discriminative undirected probabilistic graphical frame. It is utilized to encode known connections amongst perceptions and make steady Interpretations. It is habitually utilized for naming or parsing of sequential information, for example, common dialect content or natural Sequences and in PC thought. In particular, CRFs discover applications in low parsing, named substance acknowledgment and quality finding, among different errands, being a contrasting option to the related concealed Markov models. In PC thought, CRFs are regularly utilized for protest acknowledgment and picture division.

III. CHALLENGES

It is important intrusion detection must notice attacks at a premature stage in order to minimize their collision. The major challenges and requirements for building intrusion detection systems are:

The system must be able to detect as many attacks as possible lacking giving false alarms. The system must be able to handle large amount of data without disturbing performance and without sinking data. A system must not only detect an attack, but also able to classify the type of attack. A system must be resistant to attacks since, a system that can be broken during an attack may not be able to detect attacks constantly. The challenge is to build a system which is scalable and can be easily adapted as per the specific requirements of the environment where it is deployed.

IV. ANOMALY DETECTION

Intrusion Detection System assumes key part of recognizing different sorts of assaults and secures the applications and systems in the inescapably associated arrange condition. Interruption discovery is the strategy for observing PCs or systems for unapproved get to, movement, or record change. Peculiarity based IDS set up a standard of ordinary utilization examples, and anything that normally strays from it gets hailed as a conceivable interruption [10]. Abnormality identification technique can examine client examples, for example, profiling the projects executed day by day or the private procedures executed with access to assets that are inaccessible to customary client.

Analysis of Activities

The analysis is the heart of the anomaly intrusion detection system. In this system we investigate user patterns, such as profiling the programs executed on a daily basis or the privileged processes executed with admittance to resources that are inaccessible to ordinary user. For this we collect the volatile data from the system. To collect this data we use system log file

which gives us the number of processes which are running on the system, the number of resources which are assigned to the user, and the system privileged.

Prevention of Anomalous Activity

Once the anomalous activity occurs, we can prevent it. The admin may log on to the system locally or remotely. If the admin is at local level then he/she can view the running activities, or he/she can stop the anomalous activity and if the admin is at remote level then he/she can log on to the system using Internate or GPRS using cell phone. After that the user can stop anomalous activity, or start new activity. But if the controlling of the anomalous activity is not possible then admin may shutdown or reboot that system. Intrusion detection is the method of monitoring computers or networks for illegal entrance, activity, or file alteration. IDS protect a network and attempt to prevent intrusions.

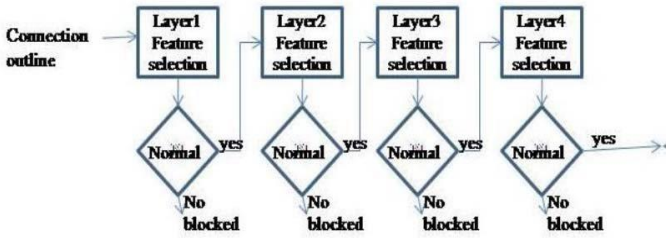

Figure 2. Layered security model

They don't fully assurance security, but when used with security procedure, susceptibility assessments, data encryption, user authentication, access control, and firewalls, they can greatly develop network safety. Intrusion detection systems provide three essential security functions: they monitor, detect, and respond to unauthorized activity by company insiders and outsiders. Intrusion detection systems use policies to term certain events that, if detected will issue an alert.

V. PIPELINING OF LAYERS

Layered security model

Layered security model is a sequential model in which number of security checks are performed one after other in sequence. Sequential Layered Approach and is based on ensuring accessibility, secrecy, and reliability of data and services over a network. The objective of using a layered security model is to condense computation and the generally time required detecting abnormal events. This can be achieved by making the layers independent to block an attack without the need of a central decision maker. In model every layer is trained separately and then deployed successively. We define four layers that correspond to the four attack groups. They are Probe layer, DoS layer, R2L layer, and U2R layer.

Pipelining

Pipelining is used by virtually all modern multicore processors to enhance performance by overlapping the execution of instructions. Proposed Pipelined Layered Security Model The layered security model improves the intrusion detection system performance by finding attacks in four layers. If the attack is found in initial layer then it is blocked otherwise test instance is passed to next layer. If the test instance is passed through all the four layers then it indicates there is no attack. In this technique the test instance is passed sequentially through all the layers. Only one test instance is checked at a time. Next instance has to wait until the previous instance completes its checking through all layers.

VI. FEATURE SELECTION FOR EACH LAYER

We first select four layers corresponding to the four attack groups those are Probe, DoS, R2L, and U2R; and perform feature selection for each layer. We illustrate our approach for selecting features for every layer and why some features were chosen over others.

Denial of Service Layer

Denial of Service attack (DoS) is an attack in which the attacker makes some computing or reminiscence source too busy or too full to hold genuine requests, or denies legitimate users access to a machine [11]. Therefore, for the DoS layer, traffic features such as the "component of links having similar object host and related service" and packet level features such as the "source bytes" and "percentage of packets with errors" is considerable. To spot DoS attacks, it may not be vital to know whether a client is "logged in or not."

Probe Layer

Probing attack is an attempt to gather information about a network of computers for the apparent purpose of circumventing its security controls Therefore, essential connection level features such as the "duration of connection" and "source bytes" are important while features like "sum of files creations" and "sum of files accessed" are not ordinary to provide information for detecting probes.

User to Remote Layer

User to Remote attack is a class of utilize in which the attacker starts out with access to a regular user account on the system and is able to exploit some vulnerability to gain root access to the system.

Remote to Local Layer

Remote to Local attacks occurs when an attacker who has the ability to send packets to a machine over a network but who does not have an account on that machine exploits some susceptibility to gain restricted access as a user of that machine.

VII. PROPOSED SYSTEM

In our proposed system we depict the Layer-based Intrusion Detection System. The LIDS draws its inspiration from what we call as the Airport Security model, where a quantity of security checks are performed one behind the other in a series. Similar to this model, the LIDS represents a sequential Layered Approach and is based on ensuring accessibility, secrecy, and integrity of data and (or) services over a network [12]. The purpose of using a layered model is to trim down computation and the generally time required detecting Anomalous events. The time required to detect an interfering event is important and can be reduced by eliminating the communication slide among different layers [13]. We classify four layers they are Probe layer, DoS layer, R2L layer, and U2R layer. Every layer is separately trained with a small set of characteristics. The layers basically act as filters that chunk any anomalous connection, thereby eliminating the need of advance processing at subsequent layers enabling quick response to intrusion [14]. The effect of such a sequence of layers is that the anomalous events are known and blocked as soon as they are detected. Just the once the attack is detected, it is intimated through mobile phone to the system administrator for secure guarding the server system [15]. We realize the LIDS and select four set of features which reduces the computational period. Methods such as naive Bayes assume independence among the observed data. To balance this trade-off, we use the CRFs that are more perfect, though pricey; however we execute the Layered Approach to improve overall system performance.

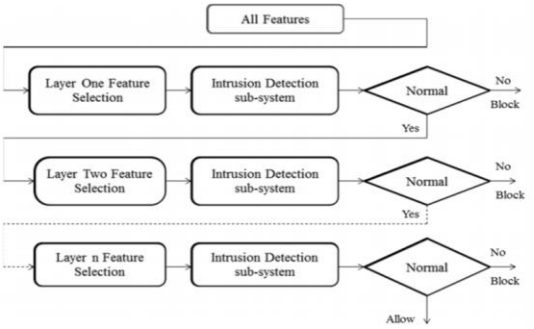

Figure 3. Feature of layers

Our proposed system, Layered CRFs, performs drastically superior than last systems.

Proposed Algorithm:

Step 1: Choose the number of layers, n, for the whole system.

Step 2: Separately execute nature selection for each layer.

Step 3: Plug in the layers sequentially such that only the connections categorized as regular are passed to the next layer

Step 4: For every (next) test instance perform Steps 5 through 8.

Step 5: Test the case and label it whichever as attack or normal.

Step 6: If the instance is labelled as an attack, block it and then identify it as an attack with the corresponding Layer name at which it is detected and go to step 4. Pass the sequence to next layer.

Step 7: If the present layer is not the last layer in the system, test the occurrence and go to step 6.Else go to step 8.

Step 8: Test the instance and label it any as normal or as an attack. If the instance is considered as an attack, block it and identify it as an attack related to the layer name.

Step 9: If the instance is considered as an attack at any layer then near it to system admin's mobile with a corresponding appropriate message of attack.

VIII. CONCLUSION AND FUTURE WORK

Hybrid intrusion detection is a novel kind of model combining the advantages of anomaly based intrusion detection and signature based intrusion detection. Intrusion and anomaly are two different kinds of uncharacteristic traffic events in an open network environment. An intrusion takes place when an unlawful access of a host computer system is attempted. A glitch

is observed at the network connection level. Both attack types may compromise important hosts, disclose sensitive data, deny services to genuine users, and pull down network based computing resources. The intrusion detection system offers intellectual protection of networked computers or distributed resources much better than using fixed rule firewalls. Existing IDSs are built with any signature-based or anomaly-based systems. Signature matching is based on a misuse model, whereas anomaly detection is based on a normal use model. However, the signature-based IDS cannot detect mysterious attacks without any recollected signatures or lack of hit classifiers. The Hybrid Intrusion Detection System integrates the litheness of Anomalous Detection System with the exactness of a signature-based Intrusion Detection System. Anomalous Detection System is planned by acquiring the unpredictable data when there is no any anomalous activity. Here we train our system using conditional random field for the anomalous activity. This new approach mechanically enables HIDS to detect related anomalous attacks in the future.

IX. REFERENCES

[1]. KK Gupta, B Nath and K Ramamohanarao, "Layered approach using conditional random fields for intrusion detection", IEEE Transactions on Dependable and Secure Computing, vol. 7, no. 1, (2010), pp. 35-49.

[2]. S Mukherjeea and N Sharma, "Intrusion Detection using Naive Bayes Classifier with Feature Reduction", Procedia Technology, vol. 4, (2012), pp. 119-128.

[3]. SJ Horng, MY Su, YH Chen, TW Kao, RJ Chen, JL Lai and CD Perkasa, "A novel intrusion detection system based on hierarchical clustering and support vector machines", Expert Systems with Applications, vol. 38, (2011), pp. 306-313.

[4]. J Vlcek and L Luksan, "Generalizations of the limited-memory BFGS method based on the quasiproduct form of update", Journal of Computational and Applied Mathematics, vol. 241, (2013), pp. 116- 129.

[5]. Li, J Xia, S Zhang, J Yan, X Ai and K Dai, "An efficient intrusion detection system based on support vector machines and gradually feature removal method", Expert Systems with Applications, vol. 39, no. 1, (2012), pp. 24-430.

[6]. V Bolón-Canedo, N Sánchez-Maroño and A Alonso-Betanzos, "Feature selection and classification in multiple class datasets: an application to KDD Cup 99 dataset", Expert Systems with Applications, vol. 38, no. 5, (2011), pp. 5947- 5957.

[7]. W Alsharafat, "Applying Artificial Neural Network and eXtended Classifier System for Network Intrusion Detection", The International Arab Journal of Information Technology, vol. 10, no. 3, (2013), pp. 230-238.

[8]. L Zhang, LG Meng and CJ Hou, "Intrusion Detection Based on Immune Principles and Fuzzy Association Rules", Intelligence Computation and Evolutionary Computation, vol. 180, (2013), pp. 31- 35.

[9]. C Guo, YJ Zhou, Y Ping, ZK Zhang, GL Liu and YX Yang, "A distance sum-based hybrid method for intrusion detection". Appl Intell, vol. 40, (2014), pp. 178-188.

[10]. SANS Institute, (2012) Intrusion Detection FAQ.http://www.sans.org/resources/idfaq/ Autonomous Agents for Intrusion Detection, http://www.cerias. purdue.edu/research/aafid/, 2010.

[11]. Kapil Kumar Gupta, Baikunth Nath, Senior Member, IEEE, and Ramamohanarao Kotagiri, Member, IEEE, ―Layered Approach Using Conditional Random Fields for Intrusion Detection‖, ieee transactions on dependable and secure computing, vol. 7, no. 1, January -march 2010

[12]. CRF++: Yet another CRF Toolkit, http://crfpp.sourceforge.net/, 2010.