

An Hybrid approach for Intrusion Detection

By

Dr Akash Saxena¹, Ramesh Soni ²

Associate Prof, S.J College of Engineering and Technology , Dausa (RAJ)¹

Research Scholor, Jodhpur National University, Jodhpur (RAJ) ²

akash27saxena@gmail.com

ABSTRACT

Now a day's security in network has become very important issue in network. Hackers and intruders are trying to crack the systems of various organizations. Intrusion detection has traditionally been performed at the operating system level by comparing expected and observed system resource usage. Gradually with time network intrusion detection came into existence .And thereafter an age of Data Mining came, which lead to evolution of many ideas in intrusion detection. Many algorithms like A-Priory algorithm were used in network to avoid hackers into the network.

A new approach has been proposed in which anomaly detection takes place with the help of two approaches called FP-Growth and Registry Anomaly Detection which made the Intrusion Detection System much more efficient and Accurate as compared to the existing System.

Keywords

IDS, internal intruder, external intruder

1. INTRODUCTION

Security is a big issue for all networks in today's enterprise environment. Hackers and intruders have made many successful attempts to bring down high-profile company networks and web services. [10]Many methods have been developed to secure the network infrastructure and communication over the Internet, among them the use of firewalls, encryption, and virtual private networks. [11]An Intruder attempts to gain, or already gained unauthorized access to the system. The intruder can either be an insider or an outsider.

Internal intruder means the intruder who has the permission to use the computer with normal user privileges. These intruders use a hole in some of the operating systems to escalate their privilege level whereas External intruder is an intruder who is on some another network and tries to exploit vulnerability in an unprotected network services on the computer to gain unauthorized entry and control. External intruders do not have any authorized access to the system they attack.[9]

Data mining plays an important role in current era of intrusion detection systems it collects data from sensors which monitor some aspect of a system. Sensors may monitor network activity, system calls used by user processes, or file system

access. They extract predictive features from the raw Data stream being monitored to produce formatted data that can be used for detection. Data gathered by sensors is evaluated by a detector using a detection model. This model determines whether or not the data is intrusive. Algorithms for building detection models are usually classified into two categories i.e Misuse detection and Anomaly detection.[8]

Misuse detection algorithms model known attack behavior. They compare sensor data to attack patterns learned from the training data. If the sensor data matches the pattern of some known attack data, the observed data is considered intrusive. Misuse models are typically obtained by training on a large set of data in which the attacks have been manually labeled. This data is very expensive to produce because each piece of data must be labeled as either normal or some particular attack on the other hand Anomaly detection models compare sensor data to normal patterns learned from the training data. If the sensor data deviates from normal behavior, the anomaly detection model classifies the data as to have originated from an attack. Anomaly detection models are popular because they are seen as a possible approach to detecting unknown or new attacks.

2. LITERATURE REVIEW

1. A Novel Rule-based Intrusion detection System Using Data Mining
For discovering user behaviour pattern, data mining and machine learning technology has been applied into network traffic data. Association rules and sequence rules are the main techniques of data mining for intrusion detection. Association rule gives the frequent itemset after that, use sequence rules for findout missing data sets. [1]
2. A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems
This paper designed a standard corpus to evaluate both false alarm rates and detection rates of intrusion detection systems using many types of both known and new attacks embedded in a large amount of normal background traffic[2].

3. Design of Intrusion Detection Model Based on FP-Growth and Dynamic Rule Generation with Clustering

In this paper author designed a framework for measure the performance of intrusion detection system based on Detection Rate (DR), False Positive Rate (FPR) and False Negative Rate (FNR). To implement this firstly K- Means clustering is apply for separation of similar and dissimilar elements and after that association rule mining is used for better detection.[3]

4. A comparative evaluation of two algorithms for windows registry anomaly detection

In this paper author presented a host-based intrusion detection system (IDS) for Microsoft Windows. This system not only enable to detect attacks on a host by accesses window registry also compares two anomaly detection algorithms like Probabilistic Anomaly Detection and Support Vector Machine and then evaluate their performance.[4]

5. Network Intrusion Detection

In this paper author design an intrusion detection system using association rules on network audit data. It finds unusual behavior that that compromises the integrity, confidentiality, and availability of information resources. In this method firstly algorithm is implemented on an item sets from the training set after that rule built by item sets and further tested on the data set. This intrusion detection system would display the item set against attacks that allows the user or administrator to filter out those unnecessary item sets and concentrate on those item sets that produce more accurate results.[5]

6. A General Study of Associations rule mining in Intrusion Detection System

This paper had shown an intrusion detection system on audit data. In this system to calculate frequent patterns apply data mining algorithm that is fuzzy association rule mining after that apply a classification algorithm to detect intruder. This system is more efficient than other association rule used system because it used association rule with negations and with varying support threshold.[6]

3. PROPOSED WORK

In our proposed work we here tried to hybrid the FP-tree Algorithm and RAD algorithm to make a better approach for anomaly detection, which are shows in figure 1. Basically we have tried to apply FP-Tree algorithm on RAD algorithm. Also we have tried to put RAD algorithm on LAN i.e. we have tried to convert the application of RAD Algorithm from Host Based Intrusion Detection System to Network Based Intrusion Detection System. RAD Algorithm is nothing but Registry Anomaly Detection Algorithm. In this basically window registry of a particular system is checked and it is examined that what work has been done on a system. It is also checked whether the work done by the user on the system is authorized or not. Basically with the help of RAD Algorithm we can monitor the work done by the user. And on the basis of it, it is decided that whether any malicious activity is

performed or not. Not only this it can also find out the malicious work done by the unauthorized user.

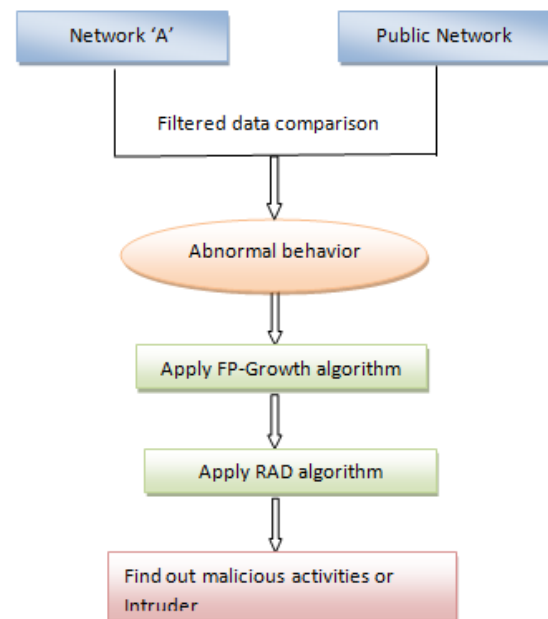


Figure 1: Block Diagram of Hybrid technique of Anomaly detection using pattern matching

4. CONCLUSION

Using the two approaches we have tried to develop a system which not only detects the intrusion on the basis of user id, password, ip address but also on the basis of work done by the system during that period. Here the two approaches used are Registry Anomaly Detection and FP-Growth Algorithm. Since these two algorithms are considered to be a good approach in their own fields, we have tried to combine them, took their strong points and tried to combine them to make a better and more efficient algorithm.

FP-Growth algorithm is used to calculate the number of times a particular user is using a particular IP address. RAD algorithm is based on checking window registry, which keeps the information about the work done by the system.

For counting we have used FP-Growth algorithm because which transforms a database into FP-tree stored in main memory using just 2 database scans, and then performs mining on that optimized FP-tree structure. Frequent pattern mining is often regarded as advanced querying where a user specifies the source dataset, the minimum support threshold, and optionally pattern constraints within a given constraint model. With the use of FP Growth algorithm, we can reduce the complexity of the system and no. of scans. This in turn reduces the time for searching and as a result makes the system fast.

5. REFERENCES

- [1] Lei Li, De-Zhang Yang, Fang-Cheng Shen, "A Novel Rule-based Intrusion detection System Using Data Mining" international conference 2010.
- [2] K. Kendall "A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems, M. Eng.Thesis" Massachusetts Institute of Technology, Massachusetts, United States, June 1999.
- [3] Manish Somani, Roshni Dubey, "Design of Intrusion Detection Model Based on FP-Growth and Dynamic Rule Generation with Clustering", International Journal of Advanced Computer Research, Volume-3 Number-2 Issue-10 June-2013
- [4] Salvatore Stolfo, Frank Apap, "A comparative evaluation of two algorithms for windows registry anomaly detection", 2005
- [5] Flora S. Tsai, "Network Intrusion Detection", International Journal of Recent Trends in Engineering, Vol 2, No. 2, November 2009
- [6] Vikas Markam, Shirish Mohan Dubey, "A General Study of Associations rule mining in Intrusion Detection System", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 1, January 2012
- [7] Qingqing Zhang, Hongbian Yang, Kai Li, "Research on the Intrusion Detection Technology with Hybrid Model", 2nd Conference on Environmental Science and Information Application Technology, 978-1-4244-7388-5/10, ESIAT, pp. 646-649, 2010
- [8] Mingle Intrusion Detection System Using Fuzzy Logic", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-3, February 2013.
- [9] Efficient parallel Data Mining with the Apriori Algorithm on FPGA's by Zachary K. Prasanna (2005)
- [10] Detection Systems as Evidence Peter Sommer Computer Security Research Centre, London School of Economics & Political Science P.M.Sommer@lse.ac.uk (2000)
- [11] [Http://wiki.answers.com/Q/What_are_the_three_types_of_intruders?#slide=1](http://wiki.answers.com/Q/What_are_the_three_types_of_intruders?#slide=1)