ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Implementation of Online Network Attack Detection in Absence of Previous History of Attack

Snehal P. Chincholkar[*1], Prof. P.D.Gawande[2]

[*1,2]Department of Electronics and Telecommunication Engineering , Sipna College of Engineering and Technology, Amravati, Maharashtra, India

snehalchincholkar@yahoo.in

Abstract

Security is demand of today's internet users. As the no. of internet users are increasing day by day it is being a paramount task to provide a network security. In the field of security NIDS acts as war horses. These NIDS are nothing but the softwares that are used to detect the network attacks. In this paper we are providing the technique that will detect the network attack without having any previous knowledge about the attack. This technique will be proved as the milestone in NIDS as these systems are useful in detecting the attacks in completely unsupervised manner. This technique uses the online basis to detect the attack that is by using the technique of multiresolution flow aggregation traffic is captured online and then by using clustering techniques filtering rules are formed to filter the network attacks from violating the security of network. All this process happens without having previous knowledge about the attack hence the name online network attack detection in absence of previous history of attack that is unsupervised network intrusion detection is true.

Keywords : NIDS, unsupervised, multiresolution flow aggregation, clustering techniques.

Introduction

We always define communication as transfer of information from source to destination. But when there are more than one source and destination in existence, the main question arises about security. Today number of internet users is tremendous due to this large research work is going on making the communication of internet users as safe as possible. In this paper I have made a sincere try to provide a technique for intrusion detection that will be proved as milestone in NIDS i.e. Network Intrusion Detection Systems.

An intrusion detection system (IDS) is software that automates the intrusion detection process. If we analyze the network attack detection systems they are categorized into two basic parts one is misuse detection that means detecting the attack which is previously known and another is anomaly detection which means that detection of such anomalies which are not previously happened.

Signature-based detection systems are highly effective to detect those attacks which they are programmed to alert on. Traditional Network Intrusion Detection Systems (NIDSs) rely on either specialized signatures of previously seen attacks, or on expensive and difficult to produce labeled traffic datasets for user-profiling to hunt out network attacks. Despite being opposite in nature, both approaches share a common downside: they require the knowledge provided by an external agent, either in terms of signatures or as normal-operation profiles. Anomaly detection uses labeled data to build normal-operation-traffic profiles, detecting anomalies as activities that deviate from this baseline. Such methods can detect new kinds of network attacks not seen before.

UNADA, is an Unsupervised Network Anomaly Detection Algorithm for knowledge-independent detection of anomalous traffic. UNADA uses a novel clustering technique based on Sub-Space-Density clustering to identify clusters and outliers in multiple low-dimensional spaces. The evidence of traffic structure provided by these multiple clustering is then combined to produce an abnormality ranking of traffic flows, using a correlation-distance-based approach.

The structure of the anomaly identified by the clustering algorithms is used to automatically construct specific filtering rules that characterize its nature, providing easy-to-interpret information to the network operator. In addition, these rules are combined to create an anomaly signature, which can be directly exported towards standard security

ISSN: 2277-9655
Impact Factor: 1.852

devices like IDSs, IPSs, and/or Firewalls. The clustering algorithms are highly adapted for parallel computation, which permits to perform the unsupervised detection and construction of signatures in an online basis

Methodology

Actually there are two methods for detecting the network attacks. One is signature based that is detecting the attack in terms of the known attack and another is without having any previous knowledge about the attacks that is UNADA.

In this project we are going to use the concept of UNADA. UNADA, is an Unsupervised Network Anomaly Detection Algorithm for knowledge-independent detection of anomalous traffic.

The structure of the anomaly identified by the clustering algorithms is used to automatically construct specific filtering rules that characterize its nature, providing easy-to-interpret information to the network operator. In addition, these rules are combined to create an anomaly signature, which can be directly exported towards standard security devices like IDSs, IPSs, and/or Firewalls. The clustering algorithms are highly adapted for parallel computation, which permits to perform the unsupervised detection and construction of signatures in an online basis.

The procedure starts with collecting the network traffic. For capturing this network traffic we have used the software named as “Network Active PIAFCTM” . This software generates the log file when it is operated in packet mode. The contains of log file are

1. data types, 2.no. of bytes transferred, 3.source IP, 4desination IP, 5.SOURCE Port, 6destination port, 7.time

TCP	62	192.168.1.100	192.203.56.67	2192	80 [2012.03.23 - 20:14:16.515]
TCP	54	192.168.1.100	192.203.56.67	2192	80 [2012.03.23 - 20:14:16.859]
TCP	62	192.203.56.67	192.168.1.100	80	2192 [2012.03.23 - 20:14:16.859]
TCP	814	192.168.1.100	192.203.56.67	2192	80 [2012.03.23 - 20:14:16.859]
UDP	307	192.168.1.1	239.255.255.250	2049	1900 [2012.03.23 - 20:14:16.890]
UDP	316	192.168.1.1	239.255.255.250	2049	1900 [2012.03.23 - 20:14:17.000]
UDP	379	192.168.1.1	239.255.255.250	2049	1900 [2012.03.23 - 20:14:17.093]
UDP	371	192.168.1.1	239.255.255.250	2049	1900 [2012.03.23 - 20:14:17.203]
TCP	994	192.203.56.67	192.168.1.100	80	2192 [2012.03.23 - 20:14:17.218]
UDP	316	192.168.1.1	239.255.255.250	2049	1900 [2012.03.23 - 20:14:17.296]
TCP	54	192.168.1.100	192.203.56.67	2192	80 [2012.03.23 - 20:14:17.343]

Now our next step is to analyze this log file in particular time slots. In this paper I have used the time slot of 1 second that means I am going to analyze the complete log file in the time slot of one second. This technique is also known as multi resolution windowing technique. Here I am applying the window of 1 second means I am going to evaluate all the parameters or attributes of the log file in one second first and repeat the procedure for remaining.

The next step is to create a feature space matrix X. This feature space matrix characterizes the captured network traffic according to the time series of particular one second. The different attributes of this feature space matrix are,

1. time series,
2. No. of data bytes transferred,
3 .No.of different source IPs in one second,
4. No.of different destination IPs in one second,
5. No.of different source ports in one second,
6. No.of different destination ports in one second,
7. Data types,
8. Ratio of no. of data bytes transferred to no. of different destination ports.

The feature space matrix hence can be determined as

$X = [x_1, x_2, x_3, \ldots\ldots\ldots\ldots\ldots\ldots x_n]$

Where these x1,x2,…xn are the features for particular time series taken into account for one second only.

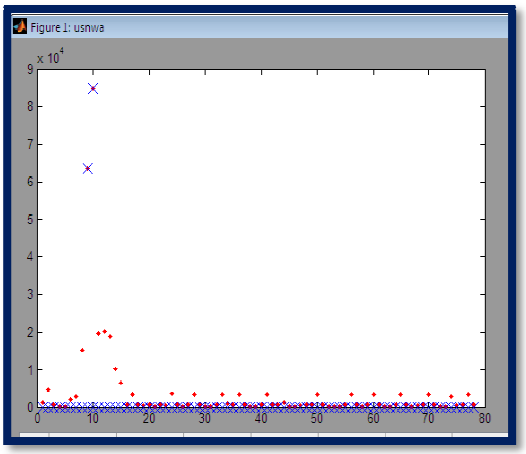
	1	2	3	4	5	6	7	8
1	1	1299	3	3	3	3	1	433
2	2	4548	3	3	3	3	1	1516
3	3	752	1	1	1	1	1	752
4	4	82	1	1	1	1	1	82

As we obtained the feature space once we are able to use clustering algorithm to detect the normal and abnormal flow from the particulars we are having with us in the feature space matrix.

The clustering algorithm is the tool used to divide complete feature space into two parts that is normal and abnormal. Here the bigger part is considered as normal one and the smaller one is considered as the abnormal part. Now this abnormal part is treated as avidance and by using the technique of evidence accumulation this smaller group is now used to create the signature for another data transferred by adding this abnormalities for filtering rules.

ISSN: 2277-9655
Impact Factor: 1.852

Result



The result of implementation of the paper is shown in the above diagram. This result is generated by using k-means algorithm which results into formation of two parts one is for normal flow and another for abnormal flow. As shown in the diagram the normal flow is denoted by dots at bottom and the abnormalities are denoted by crosses at the top of the figure indicating the abnormal flows. These abnormalities are then used as evidence for formation filtering rules for secured transmission of data afterwards.

Conclusion

Here we have proposed the new intrusion detection system which can be used for detection of network attack in online basis. This system will be proved as milestone in designing NIDS that is software used for detection of network attack. This allows detecting new previously unseen network attacks, even without using statistical learning. By combining the notions of Sub-Space Clustering and multiple Evidence Accumulation

Applications

- Applications of this project are found in defense and security areas as the different unknown attacks can be detected by using this project. For security purpose it is necessary to detect an unknown attack and hence this project is useful as this project can detect the attack without knowing the previous history of the attack.

- This project is useful for firewall construction to detect the unauthorized data. This advantage is useful in different applications in and industrial area where the unauthorized receiver may cause severe problems.
- In the area of banking this project is advantageous to detect the unauthorized transmitter or receiver of data

References

[1] *Pedro Casas, Johan Mazel and Philippe Owezarski," UNADA: Unsupervised Network Anomaly Detection using Sub-Space Outliers Ranking", UPS, INSA, INP, ISAE; LAAS; F-31077 Toulouse, France.*

[2] *Portnoy, E. Eskin, and S. Stolfo, "Intrusion Detection with Unlabeled Data Using Clustering", in Proc. ACM DMSA Workshop, 2001.*

[3] *M. Thottan and J. Chuanyi, "Anomaly Detection in IP Networks", in IEEE Trans. Sig. Proc., vol. 51 (8), pp. 2191-2204, 2003.*

[4] *Rui Xu, Student Member, IEEE and Donald Wunsch II, Fellow, IEEE, "Survey of Clustering Algorithms", IEEE TRANSACTIONS ON NEURAL NETWORKS, VOL. 16, NO. 3, MAY 2005*

[5] *S. Hansman, R. Hunt "A Taxonomy of Network and Computer Attacks",in Computers and Security, vol. 24 (1), pp. 31-43, 2005*

[6] *A. Fred and A. K. Jain, "Combining Multiple Clusterings Using Evidence Accumulation", in IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 27 (6), pp. 835-850, 2005*

[7] *Anna Sperotto, Gregor Schaffrath, Ramin Sadre, Cristian Morariu, Aiko Pras and Burkhard Stiller," An Overview of IP Flow-Based Intrusion Detection", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 12, NO. 3, THIRD QUARTER 2010.*

[8] *Pedro Casas , Johan Mazel, and Philippe Owezarski ," Steps Towards Autonomous Network Security: Unsupervised Detection of Network Attacks ", IEEE 2011 .*

[9] *Pedro Casas, Johan Mazel, and Philippe Owezarski, CNRS and Université de Toulouse," Knowledge-Independent Traffic Monitoring: Unsupervised Detection of Network Attacks", IEEE Network January/February 2012*