A Survey of Signature Based & Statistical Based Intrusion Detection Techniques

Manu Bijone[1] Jitendra Dangra[2]
[1]M.Tech Student [2]Assistant professor
[1]Department of Computer Science and Engineering
[2]Department of Information and Technology Engineering
[1,2]Lakshmi Narain College of Technology, Indore, India

Abstract— This paper presents a comprehensive survey of some modern and most popular intrusion detection techniques. It is unrealistic to prevent security breaches completely using the existing security technologies. Detecting the presence of intruder is very crucial for maintaining the network security. It is found that most of the current intrusion detection systems (IDSs) are signature based systems. The signature based intrusion detection system are based on matching a signature with the network details. Provided with the signatures or patterns they can detect many or all known attack patterns but they are of little use for as yet unknown attacks. Rate of false positives is close to nil but these types of systems are poor at detecting new attacks or variation of known attacks or attacks that can be masked as normal behavior. The other type of IDS i.e. Statistical Based Intrusion detection System (SBIDS) can overcome many of the aforementioned limitations of signature based intrusion detection systems. The statistical based intrusion detection systems performs better than signature based intrusion detection system for novelty detection i.e. detection of new attack is very important for intrusion detection system. Researchers have implemented various classification algorithms for intrusion detection.

Key words: SBIDS, IDSs

I. Introduction

Over the years the intrusion detection has become one of the most popular field of research. The main reason is that most of the organizations have become automated & they also make use of the internet & the network technology for the transmission of the data. So it is clear that the security of the data sent & receive has become trivial. To avoid the intruders to fetch the all important data, there is a need of some kind of mechanism which can prevent this unauthorized access. The data mining techniques plays a vital role in intrusion detection systems. These techniques have the capability to deal with the voluminous data.

A. Network Based IDS:

Because they only scrutinize network traffic [1], the NIDS do not benefit from running on the host. They are often run on dedicated machines that observe the network flows sometimes in conjunction with a firewall. That's why the security threats of the clients do not affect the monitors.

One major shortcoming of NIDS is that they are oblivious to local root attacks. The authorized user of the system that attempts to gain additional privileges will not be deleted if attack is performed locally. The authorized user of the system may be able to set up an encrypted channel when accessing the machine remotely.

B. Host Based IDS:

The HIDS have an ideal vantage point [1,3]. An HIDS runs on the machine it monitors, HIDS can theoretically observe and log any event occurring on the machine.

It means that an HIDS can only be trusted up to the point where the system was compromised. As network attacks have increased in number severity over the past few years, intrusion detection system (IDS) is becoming a critical component to secure the network. Because of large volumes of security audit data as well as complex and dynamic properties of intrusion behaviors, the optimization of the performance of IDS becomes an important open problem that is receiving more and more attention from the research community. Uncertainty to explore if certain algorithms perform better for certain attack classes constitutes the motivation for the reported herein.

The Data mining-based intrusion detection systems(IDSs) have demonstrated high accuracy, also good generalization to novel types of intrusion and robust behavior in a changing environment in recent years. A major problem faced by them is the intensive computation required in the model generation phase.

II. Literature survey

In [6] Jake Ryan et al has worked on the concept of the neural network. The neural network performs learning on the basis of the test data and then it performs predictions. It can classify that the behavior of the node as normal or abnormal.

Denning D.E et al [7, 8] has presented a sequential rule based model for the prediction of abnormal behavior. Sequential rules are based on the sequential data base. The training data is stored in the sequence in which hey occur in the sequence data set & then the sequence rule mining algorithm is applied on the training data set to identify the patterns of the normal behavior and the abnormal behavior. The system developed in [9] has more accuracy in identifying whether the records are normal or attack one.

Dewan M et al [10] proposed an improved version of the self adaptive Bayesian algorithm (ISABA). It is based on the concept of the Bayesian network but accuracy rate is below expectation.

S.Sathyabama et al [11] presented a method based on the clustering. In this method the similarity based records are stored in the clusters. Also the dissimilar records are called the outliers. For the outliers the alarm is raised & the record is checked for the abnormal behavior.

Amir Azimi Alasti et al [12] proposed a self organizing map based method for the intrusion detection. The map has been used successfully to classify the data records .

in this method the false positive alerts have been reduced up to a good extent.

Alan Bivens et al [13] has proposed a self organizing map based classification technique. The false negative has been reduced in this model.

The authors of [14] proposed the ensemble approach. This approach is a fusion of many existing algorithm. The experimental results have shown that it has outperformed many existing techniques. It has also outperformed support vector machine.

This paper [15] presents a method which is based on the concept of the dimension reduction. The dimension reduction is achieved by the feature extraction technique of the data mining.

Aly Ei-Senary et al [16] has proposed a fusion of the apriori and the kuok algorithm. This proposed model also uses the concept of the fuzzy set i.e. partial membership function.

Taeshik Shon et al [17] proposed a novel framework. This novel framework contains the updated support vector machine. It also performs the packet profiling. The concept of clustering is also applied in brief. Overall it is a very complex process.

In this paper [18] the author has proposed a genetic algorithm based intrusion detection system. The accuracy is better but the solution is not guaranteed at all.

Oswais.S et al [2] also proposed genetic algorithm based IDS. The GA is used to udate the membership function. It also contains a detailed survey of the IDS.

Norouzian M.R et al [4] defined Multi- Layer Perceptron (MLP) based technique for the intrusion detection and classification. The backpropagation algorithm has been used for the error rate deduction. The work done in [5] also proposes a GA and clusting based method for the IDS.

Lunt, T.F., 1988 [19] , a survey of intrusion detection expert system is proposed. The proposed method is fusion of two methods to create a strong intrusion detection system.

Todd Heberlein [20] proposed an intrusion detection system called network system monitor. This system is based on the concept of analyzing network instead of the system log entry.

Teng, Chen, And Lu [21], proposed time based inductive machine to capture or store user behavior. Inductive generalization is also a part of the process.

Anderson D, Lunt TF, Javitz H, Tamaru A, Valdes [22], proposed a network intrusion detection expert system. This system learns from the training data and predicts the test data.

Lane and Brodley [23] applied the concept of the instant based learning. Lee W. and Stolfo S. and Mok [24] proposes a novel data mining based framework for intrusion detection. This model is based on the concept of the utilizing the contents of the audited programs.

Debar, H., Dacier, M., And Wespi [25] proposes taxonomy of the intrusion detection systems. This classification is done according to the property of the intrusion detection system. Axelsson, S [26] also proposed a taxonomy of the IDS. They also presented the background details of some IDS. Yu Chen, Yu-Kwong Kwok [27] proposed a novel signal processing based intrusion detection system.

III. Conclusion

Intrusion is harmful for the data flowing on the internet. Intrusion reduces the authenticity. To make sure that the information or data is secure from the unauthorized access, the IDS is must. It identifies the system, which is performing malfunctioning. In this paper, the comprehensive survey over the most effective and most popular intrusion detection system has been performed. Each methods working together with the related merits and demerits has been discussed. This literature review will help other researchers in their further research or study.

References

[1] Litty Lionel, “Hypervisor-based Intrusion Detection”, Master of Science Graduate department of computer Science University of Torronto, 2005.

[2] Sadiq Ali Khan, “Rule-Based Network Intrusion Detection Using Genetic Algorithm”, International Journal of Computer Applications, No: 8, Article: 6, 2011, DOI: 10.5120/2303-2914.

[3] Norouzian.M.R, Merati.S, “Classifying Attacks in a Network Intrusion Detection System Based on Artificial Neural Networks”, in the Proceedings of 13th International Conference on Advanced Communication Technology(ICACT), 2011,ISBN:978-1-4244-8830-8,pp-868-873.

[4] Jin-Ling Zhao, Jiu-fen Zhao ,Jian-Jun Li, “Intrusion Detection Based on Clustering Genetic Algorithm”, in Proceedings of International Conference on Machine Learning & Cybernetics (ICML),2005, IEEE Communication Magazine,ISBN:0-7803-9091-1,DOI: 10.1109/ICML.2005.1527621.

[5] Anderson.J.P, “Computer Security Threat Monitoring & Surveilance”, Technical Report, James P Anderson co., Fort Washington, Pennsylvania, 1980.

[6] Jake Ryan, Meng - Jang Lin, Risto Miikkulainen, ”Intrusion Detection With Neural Networks”, Advances in Neural Information Processing System 10, Cambridge, MA:MIT Press,1998,DOI:10.1.1.31.3570.

[7] Denning .D.E, ”An Intrusion Detection Model”, Transactions on Software Engineering, IEEE Communication Magazine, 1987,SE-13, PP-222-232,DOI:10.1109/TSE.1987.232894.

[8] Teng.H.S, Chen.K and Lu.S.C, “Adaptive Real-Time Anomaly Detection using Inductively Generated Sequential Patterns, in the Proceedings of Symposium on research in Computer Security & Privacy, IEEE Communication Magazine,1990, pp-278-284.

[9] Sekeh.M.A,Bin Maarof.M.A, “Fuzzy Intrusion Detection System Via Data Mining with Sequence of System Calls”, in the Proceedings of International Conference on Information Assurance & security (IAS)2009,IEEE Communication Magazine, pp- 154-158,ISBN:978-0-7695-3744-3,DOI:10.1109/IAS.2009.32.

[10] Dewan Md, Farid, Mohammed Zahidur Rahman, “Anomaly Network Intrusion Detection Based on Improved Self Adaptive Bayesian Algorithm”, Journal

of Computers, Vol 5, pp-23-31, Jan 2010, DOI:10.4.304/jcp 5.1.

[11] Sathyabama.S, Irfan Ahmed.M.S, Saravanan.A,"Network Intrusion Detection Using Clustering: A Data Mining Approach", International Journal of Computer Application (0975-8887), Sep-2011, Vol: 30, No: 4, ISBN: 978-93-80864-87-5, DOI: 10.5120/3670-5071.

[12] Amir Azimi, Alasti, Ahrabi, Ahmad Habibizad Navin, Hadi Bahrbegi, "A New System for Clustering & Classification of Intrusion Detection System Alerts Using SOM", International Journal of Computer Science & Security, Vol: 4, Issue: 6, pp-589-597, 2011.

[13] Alan Bivens, Chandrika Palagiri, Rasheda Smith, Boleslaw Szymanski, "Network-Based Intrusion Detection Using Neural Networks", in Proceedings of the Intelligent Engineering Systems Through Artificial Neural Networks, St.Louis, ANNIE-2002, and Vol: 12, pp- 579-584, ASME Press, New York.

[14] Srinivas Mukkamala, Andrew H. Sung, Ajith Abraham, "Intrusion Detection Using an Ensemble of Intelligent Paradigms",Journal of Network & Computer Applications ,pp-1-15, 2004.

[15] Shilendra Kumar, Shrivastava ,Preeti Jain, "Effective Anomaly Based Intrusion Detection Using Rough Set Theory & Support Vector Machine(0975-8887), Vol:18,No:3, March 2011,DOI: 10.5120/2261-2906.

[16] Aly Ei-Semary, Janica Edmonds, Jesus Gonzalez-Pino, Mauricio Papa, "Applying Data Mining of Fuzzy Association Rules to Network Intrusion Detection", in the Proceedings of Workshop on Information Assurance United States Military Academy 2006, IEEE Communication Magazine, West Point, NY,DOI:10.1109/IAW.2006/652083.

[17] Taeshik Shon, Jong Sub Moon, "A Hybrid Machine Learning Approach to Network Anomaly Detection", Information Sciences 2007, Vol: 177, Issue: 18, Publisher: USENIX Association, pp- 3799-3821, ISSN:00200255,DOI:10.1016/j.ins-2007.03.025.

[18] Sachin Patil, Deepak Kapgate, P. S. Prasad, " Effective concept for detection of web based attacks using ID3 algorithm", IJCSMC, Vol. 3, Issue. 5, May 2014, pg.321 – 330

[19] Lunt, T. "Detecting intruders in computer systems," in Proceedings of Conference on Auditing and Computer Technology, pp. 1-17, 1993.

[20] Todd, H. L., Gihan V.D., Karl N.L., Biswanath, M., Jeff, W. and David, W. "A network security monitor," in Proceedings of Symposium on Research in Security and Privacy, Oakland, CA, pp. 296–304, 1990.

[21] Teng, H., Chen, K. and Lu, S. "Adaptive real time anomaly detection using inductively generated sequential patterns', IEEE Computer Society Symposium on Research in Security and Privacy, California, IEEE Computer Society, pp. 278-84, 1990.

[22] Anderson, J.B. and Mohan, S. "Sequential coding algorithms: A survey and cost analysis", IEEE Transactions on Communication, Vol.32, pp. 169-176, 1984.

[23] Lane, T. and Brodley, C.E. "Temporal sequence learning and data reduction for anomaly detection", ACM Transactions on Information and System Security, Vol. 2, No. 3, 1999.

[24] Lee, W., Stolfo, S. and Mok, K. "Adaptive intrusion detection: A data mining approach", Artificial Intelligence Review, Kluwer Academic Publishers, Vol. 14, No.6, pp. 533-567, 2000.

[25] Debar, H., Becker, M. and Siboni, D. "A neural network component for an intrusion detection system," in IEEE Symposium on Research in Computer Security and Privacy, pp. 240-250, 1992.

[26] Axelsson, S. Research in intrusion-detection systems: A survey, Technical Report, Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden, 1998.

[27] Yu, Z., Chen, J. and Zhua, T. "A novel adaptive intrusion detection system based on data mining," in Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, pp. 2390-2395, 2005.