International journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.1., Issue.4., 2013

RESEARCH ARTICLE

ISSN:2321-7758

A SURVEY ON INTRUSION AWARENESS TECHNIQUES

PRASHANT SHAKYA[1] , MR. RAHUL SHUKLA[2]
College of Science and Engineering, Jhansi

Article Received: 19/01/2014 | Article Revised on:29/01/2014 | Article Accepted on:01/02/2014

PRASHANT SHAKYA

ABSTRACT

Intrusion awareness system (IAS) is a security layer that is used to discover ongoing intrusive attacks and anomaly activities in information systems and is usually working in a dynamically changing environment. Although increasing IDSs are developed, network security administrators are faced with the task of analyzing enormous alerts produced from the analysis of different event streams. In this paper we present different types of intrusion awareness based on the rule classification, Data fusion and support vector machine and distributed situational awareness theory.

Keywords— intrusion, Detection, Data Fusion, Support vector machine etc

INTRODUCTION

Traditional network security devices such as Intrusion Detection Systems (IDS), firewalls, and security scanners working independently of one another, with virtually no knowledge of the network assets they are defending. This lack of information results in numerous ambiguities when interpreting alerts and making decisions on adequate responses. Network systems are suffering from various security threats including network worms, large scale network attacks, etc, and network security situation awareness is an effective way for solve these problems.

Related work

Data fusion: Data fusion techniques combine data from different sources together. The main objective of happing fusion is to produce a fused result that provides the most detailed and reliable Information possible. Fusing multiple information sources together also produces a more efficient representation of the data. Multi sensor data fusion, or distributed sensing, is a relatively new engineering discipline used to combine data from multiple and diverse sensors and sources in order to make inferences about events, activities, and situations [5]. These systems are often compared to the human cognitive process where the brain fuses sensory information from the various sensory organs, evaluates situations, makes decisions, and directs action. Among the most common examples where such systems have been developed and widely used, are military systems for threat assessment and weather forecast systems. Generally, data fusion is a process performed on multi-source data towards detection, association, correlation, estimation and combination of several data streams into one with a higher level of abstraction and greater meaningfulness. In the following we present a classification and brief description of some widely used methods, motivated by the taxonomy that was originally proposed by Hall [4].

Support vector machine

Support Vector Machine (SVM) was first heard in 1992, introduced by Boser, Guyon, and Vapnik in COLT-92. Support vector machines (SVMs) are a set of related supervised learning methods used for classification and regression [1]. They belong to a family of generalized linear classifiers. In another terms, Support Vector Machine (SVM) is a classification and regression prediction tool that uses machine learning theory to maximize predictive accuracy while automatically avoiding over-fit to the data. Support Vector machines can be defined as systems which use hypothesis space of a linear functions in a high dimensional feature space, trained with a learning algorithm from optimization theory that implements a learning bias derived from statistical learning theory. Support vector machine was initially popular with the NIPS community and now is an active part of the machine learning research around the world. SVM becomes famous when, using pixel maps as input; it gives accuracy comparable to sophisticated neural networks with elaborated features in a handwriting recognition task [2]. It is also being used for many applications, such as hand writing analysis, face analysis and so forth, especially for pattern classification and regression based applications. The foundations of Support Vector Machines (SVM) have been developed by Vapnik [3] and gained popularity due to many promising features such as better empirical performance. The formulation uses the Structural Risk Minimization (SRM) principle, which has been shown to be superior, [4], to traditional Empirical Risk Minimization (ERM) principle, used by conventional neural networks. SRM minimizes an upper bound on the expected risk, where as ERM minimizes the error on the training data. It is this difference which equips SVM with a greater ability to generalize, which is the goal in statistical learning. SVMs were developed to solve the classification problem, but recently they have been extended to solve regression problems.

D-SVM

D-SVM methodology for data classification for security and awareness of security threats. Security threats awareness a challenging task for internet technology in current scenario. The current method work some probability based function for predication of data types. In this section we modified the existing section of data classification in exiting framework. Exiting framework basically data classified on rule based technique, but the amount of traffic data increase the performance of security awareness framework compromised. And more and more false alarm generation, due to this reason admin of network faced problem. Here we proposed a hybrid classification technique for data classification D-SVM. D-SVM is a combination of data fusion and support vector machine.

D-SA

Distributed Situation awareness (D-SA) is in short knowledge of what is going on. It is conscious knowledge of what is happening, what has happened, what will happen if, and what will happen if not. But D-SA is the ability or knowledge of how to act. Since D-SA incorporates awareness it is not automatic, unconscious use of data. As part of D-SA an estimation of the quality of the awareness can be included, an estimation of its correctness and completeness. But since this can also be excluded from the concept of D-SA, it is simply termed meta-SA, to distinguish quality from content. Device models to know how some device works, or how a human will act in a given situation, are part of D-SA. Since if one knows how some fact or human will act in a situation, and then it is possible to predict what will happen, in short, to get D-SA of future states. D-SA has wide applicability in the field of intrusion awareness.

Data set

KDD CUP 99 DATA SETS

The data set used in the experiments is ‘‘KDD Cup 1999 Data[21], which is a subversion of DARPA (Defense Advanced Research Projects Agency) 1998 dataset. The KDD cup 99 dataset Includes a set of 41 features [18][19] derived from each connection and a label which specifies the status of connection records as either normal or specific attack type. These features had all forms of continuous, discrete, and symbolic, with significantly varying ranges falling in four categories. Intrinsic features of a connection, the content features, the same host features and the similar same service features. Likewise, attacks fall into four main categories DoS (Denial of Service), R2L (Remote to Local), U2R (User to Root) and Probe KDD dataset is divided into training and testing record sets. Total number of connection records in the training dataset is about 5 million records. This is too large for our purpose; as such, only concise training dataset of KDD, known as 10% was employed here, distribution of normal and attack types of connection records in 10%KDD train dataset and test data respectively have been summarized in Table 5.1 [4]. As it can be seen in Table 5.1, sample distributions for different categories of attacks in training data differ significantly from each other. One of the main contributions of this work is to overcome this issue by using different classifier for each class of data. The test data enjoys a different distribution. Moreover, the test data includes additional attack types not present in the training data which makes classifying more complicated.

CONCLUSION

Network security situation awareness system and intrusion detection is a new research domain, and it has great importance in improving abilities of responding to emergences, reducing losses of network attacks, revealing abnormally intrusions and enhancing system abilities of fighting back. In this paper we discussed the study of network security situation awareness model and intrusion awareness model. In this study we studied that D-SVM has reduced attacks than rule classification also increase percentage of successful prediction In future we have design a hybrid model combined with data fusion and neural network. In future using D-SA methodology we predict the sensitive area of network and increase percentage of successful prediction.

REFERENCES

[1] Anonymous,2012 Maximum Security, Third editionSams publications, Indianapolis, Indiana, USA

[2] Yuebin Bai, Hidetsune Kobayashi, 2003. Intrusion Detection System: Technology &DevelopmentProceedings of the17th International Conference on Advanced formation Networking and Applications(AINA'03).

[3] A Murali M Rao,2005. A Survey on Intrusion Detection Approaches, IEEE.

[4] Eric Maiwad, 2001. Network Security A Beginners Guide, Chief Technology Officer, TMH publications.

[5] S. Axelsson,2000. Intrusion Detection Systems: A Survey and Taxonomy, Technical Report 99-15Department of Computer Engineering, Chalmers University

[6] White paper, Intrusion Detection: A Survey,ch.2, DAAD19-01, NSF, 2002

[7] K. Scarfone, P. Mell, Feb. 2007. Guide to IntrusionDetection and Prevention Systems (IDPS), NISTSpecial Publication, 80

[8] R.P. Lippmann, and R.K. Cunningham, "Improving Intrusion Detection Performance Using Keyword Selection and Neural Networks," Computer Networks, 2000, pp. 597-603

[9] C. Siaterlis, and,"Towards multisensor data fusion for DoS detection"

[10] J.W. Zhuge, D.W. Wang, Y. Chen, Z.Y. Ye, and W. Zou, "A Netwrok Anomaly Detection Based on the D-S Evidence Theory," Journal of Softwoare, March 2006, pp. 463-471

[11] X.W. Liu, H.Q. Wang, Y. Liang, and J.B. Lai, "Heterogeneous Multisensor Data Fusion with Neural Network: Creating Network Security Situation Awareness," Proceeding of ICAIA'07, Hong Kong, March 2007, pp. 42-4

[12] J. Kong, "Anonymous and untraceable communications in mobile wireless networks," Ph.D. dissertation, 2004, chair-Gerla, Mario.