Analysis of Security Techniques for Detecting Suspicious Activities and Intrusion Detection in Network Traffic

FaseeUllah[1], Waqas Tariq[1], Dr. Muhammad Arshad[1], Muhammad Saqib[1], Noor Gul[2]

**[1]Department of Computer Sciences,
City University of Science &Information Technology,
Peshawar, Pakistan**

**[2]Department of Electronics Engineering,
International Islamic University, Islamabad, Pakistan**

Abstract

In Computer Network number of security techniques provide security consolation but not up to optimal security extent. There are massive attacks and efficient viruses travel across the network which incapacitates computer system and default configuration of the operating system. Preceding techniques can capture anomalous activates and previous known attacks but unknown Security attacks have learned to survive in a high secure precinct, it must be noticed by every technical person that virus has an augmenting influence, so it is very difficult to detect unknown attacks at application layer on the run time.

This study analyzes some of the best well known Intrusion detection techniques and challenging number of attacks including unknown attacks. This paper presents some of appropriate techniques which are proposed for intrusion detection and anomaly detection.

Keywords: *Security; operating system; Network intrusion detection; anomaly detection; Attacks;*

1. Introduction

Computer network is the source of transmission between the machines, important information travels across the network and on the global network (Internet) but that information is accessible [1,2]. Network has become very risky and unsecure, precarious security is provided but every internet user wants to secure concern network up to optimal and acceptable extend, any machine that is connected to the global network (Internet) directly or under another domain, it has security threats [1,3]. The security issues of preceding environment computer network and internet have become obligatory; machines connected to the network are easily assessable [2, 3].

Firewalls and routers are used to detect massive kind of virus and worms but it is possible when the virus or worm is already defined in signatures and it can also be detected when the virus is already spread [4]. In order to spot these suspicious actions we use Intrusion Detection Systems (IDSs) and Intrusion Detection System is usually categorized as misuse based system or anomaly based system [6, 7, 8, 11]. Further it can be classified as hybrid based system [10].

Intrusion Detection System (IDS) is normally practiced for identifying malicious activities and their resources. Misuse based system maintains records for description of attacks and signatures that are used to detect the attacks where anomaly based system has feature of detecting previously unknown attacks [1]. Hybrid based system perform intrusion detection by using expertise of both misuse based and anomaly based system [5, 10]. Some of appropriate techniques based on Intrusion Detection System (IDS) are analyzed in detail, in this paper we discussed advantages and shortcomings of analyzed techniques that are still in use for intrusion detection.

In the rest of this paper, section 2 describes Literature review; Section 3 describes critical review and section 4 describes conclusion and future work.

2. Literature Review

Intrusion Detection System (IDS) one of the appropriate anomaly based intrusion detection technique is Bayesian Event Classifier [6]. According to author, Intrusion Detection Systems is meant to identify the predefined intrusion attacks where unlike Intrusion Detection System (IDS) in anomaly based approach there is a chance of detecting unknown attacks [6]. In same context author has anticipated an event classification technique that is based on Bayesian networks. The technique is based on two main problems; the first problem is stated as the positive false alarm that how the decision of a particular event should be treated, whether it is a normal activity or it should be detected as anomalous activity, it was detected in a simpleminded way. The second problem was, the system was not able to differentiate the anomalous behavior caused by unusual authentic action. According to author such information can be accessed by system health monitoring [6]. Further [6] has tried to rescind these two problems by classifying the previous scenarios with the change of Bayesian network by identifying Denial of Service (DOS), Masquerader attack and unknown attacks. Author has recommended this new technique as proposed solution for anomaly based intrusion detection. Some weaknesses of this proposed solution is that, this mechanism is very complex other than that we can also risk the system performance in the proposed technique.

[7] introduces the conditional random fields technique, the technique is used in a toolkit (CRF++) [7] as a model. Author has anticipated the technique as best among the previous techniques, and defined the Conditional Random Fields (CRT) as a unique technique for task of intrusion detection [7]. In the experiment among the other techniques it was recorded a very high rate of accurate results for intrusion detection. It is also one of the best feature in [7] among other techniques that proposed technique can be used without client server environment, where number of other techniques are proposed for the client server environment (research labs etc.). The proposed technique is a directionless graphical model, it used for the task of sequence classification and labeling [7], unlike the other models which prefer joint distribution the Conditional Random Fields (CRT) model favor conditional distribution. Proposed technique also avoids the observation and label bias problems. The technique of Conditional Random Fields (CRT) was proposed by identifying twenty four altered types of enormous network attacks which were further categorized in four groups of Denial of Service (DOS), Probing, R2L (unauthorized access from a remote machine) and U2R (unauthorized access to root). The experiment was matched with two other known best techniques Decision Tree [13] and Naive Bayes [13] and the results were very efficient and effective. Weakness of proposed solution is that newly born unknown attacks cannot be detected by suggested technique.

[8] has contributed a technique based on distance measure for transforming the document and making the document presentable in form of vector space model known as K-Nearest Neighbor Text Categorization [14] Technique for anomaly based intrusion detection. The scenario is described as the grouping of text documents which are string of characters in to predefined classifications called Vector Space Model [8] and applying k-Nearest Neighbor algorithm on the model to detect the malicious activities across the network. In Vector Space Model each of the documents are represented in vector of words. The proposed technique of the author is best among the other anomaly based text categorization intrusion detection techniques like Bayesian Classifier because the proposed technique does not trust on preceding probabilities [8]. The technique was proposed by identifying malicious attack, known attacks and novel attacks, when the result was provided for identified problems; the experiment was overall good enough but there were two types of attacks that were missed; one of them were a Denial of Service (DOS) and other one was process table attack [8]. The missed attacks were behaving like a normal running process in operating system and this made impossible to detect them as a malicious activity for K-Nearest Neighbor Text Categorization algorithm. Some of weaknesses of proposed model is port based attack and process table attack.

[9] Presents the technique for high speed networks intrusion detection for LINUX environment called Stateful Intrusion Detection technique. According to author the Intrusion Detection Systems (IDSs) are programmed to capture the information about the network by the flow of IP packets; it is normally designed for 100 Mbps but the network technology is moving towards enhancement and the Gigabit Ethernet (1000 Mbps) is normally used now-a-days and mounting in network labs[9]. In order to shelter the large bandwidth environment, author has proposed a

unique technique for network intrusion detection. The proposed technique Stateful Intrusion Detection is applied to a tool which takes the desire data as an input from the network and the data is then classified into controllable size of chunks, this activity is called slicing the data [9]. This large amount of data is managed by dividing the data into manageable streams and then checked by sensors. Author has also mentioned some requirements for proposed techniques, a few of which are discussed, the technique can be applied only in gigabit environment, the intrusion detection in a proposed way can only be performed by sensors, the system will also install an approach for detection of malicious activities with defined signatures and some other requirements. The technique is proposed by identifying multistep attack, all known attacks and novel attacks. Some of the weaknesses of proposed system are expensive requirement, complex installation and dependency issues.

[10] Presents a technique for enhanced self-Adaptive Naive Bayesian Tree (NBTree) which is used for anomalous based intrusion detection. Author has presented a new learning algorithm for Naive Bayesian Tree by which the performance of Naive Bayesian Tree (NBTree) has been enhanced and the detection has been scales up for different types of known attacks, it has also recorded a decrease in the rate of false positive alarm [10]. According to author the Naive Bayesian Tree (NBTree) provide similarity to traditional recursive partitioning schemes, Naive Bayesian Tree (NBTree) is a fusion and crossbreed approach that exploits the advantages of both decision trees [13] and Naive Bayesian Classifier [13]. This amalgamation of decision tree and Naive Bayesian Tree provide Improved Self-adaptive NBTree [10]. The proposed solution takes datasets of analyzed information as input and as output it presents hybrid decision trees with Naive Bayesian classifier. The technique was proposed by identifying known network attacks and dividing them into five main classifications probing attack, denial of service, user to root and root to user. Other than these four categories fifth one was for the normal class [10]. Defining normal class it was engendered by the daily activities on browser. Some of weaknesses of proposed techniques are that the proposed technique cannot detect port based attacks and Masquerader attacks as it has provided 99. 1 to 99.9% accurate results but the result is false and it also can't detect unknown attacks.

According to [11] unlike other techniques anomaly based intrusion detection has influence of detecting novel attacks, specially denial of service attack and probing attack but beside good results of novel and other attacks detection, it generates a very huge rate of false positive alarm. Author has proposed specification based technique unlike anomaly detection it has low rate of false positive alarm it doesn't detect the novels attacks which can be detected by anomaly based intrusion detection system. To escape the faults of these two methodologies and for utilizing the efforts of both approaches at same time author has combined the anomaly detection technique within the specification based technique [11]. Author has used an external finite state automation machine to deploy the scenario, where finite state machine is programmed to take the desired statistical information as well as the desired data from network protocols and packets to maintain the statics that need to be maintaining for anomaly detection [11]. Author has proposed the technique by identifying external break attack, masquerader attack, penetration attack, leakage, Denial of Service attack and malicious use attack and suggested the proposed technique as expert in detecting email virus attack. Weakness of this proposed technique is that this mechanism is very complex to understand the technique is not very efficient to detect unknown attacks and port based attacks.

[12] Presents False Positive Alert Reduction Technique for reducing the false positive alarm rate. According to author network Intrusion Detection System (IDS) is very susceptible for identifying and detecting network attacks but whenever Intrusion Detection System predict any intrusion, it activates alarm for security alert but there are thousands of activities running across the networks; Intrusion Detection System (IDS) generates thousands of alarm on scents of suspiciousness of any particular activity, it is fact that most of them are false [12]. To avoid the discussed problems author has proposed Alert Reduction Technique. In this technique it has been recommended to update the desired patches and updates the security signatures. Author has compared this technique with sensor level and log alert technique and suggested the proposed technique among previous contribution. The technique was proposed by identifying Spoofing attack, malicious use attack, known and unknown attacks [12]. Weakness of this proposed technique is that, it cannot detect newly born unknown attacks as this attack was identified problem for proposed

solution but the results are false in case of unknown attacks.

3. Critical Review

In literature review we have seen all the existing techniques with their separate merits and demerits. In the description about the techniques used with a brief summary, identified problems, and proposed solution of critical review section we illustrate tabular representation of previous studied techniques and methods in literature review section with their complete information as shown in table 1.This information will provide a brief identified problem, reliability of technique and weaknesses or limitations of the proposed technique.

TABLE 1 SUMMARY OF VARIOUS DISCUSSED TOOLS IN LITRATURE REVIEW

Author(s)	***Name of Proposed Technique***	***Summary***	***Identified Problem(s)***	***Proposed Solution***	***Data used***	***Implemented***	***Limitations***
C. Kruegel, D. Mutz, W. Robertson & F. Valeur 2003	Bayesian Event Classifier	A Bayesian network for modeling uncertainty issues by representing parent child relations of nodes to indicate anomaly based intrusions.	Denial of service, Masquerader attack and unknown attacks	An event classification scheme applying on Bayesian network	YES	YES	Complex mechanism can't be used for a standalone machine.
K. K. Gupta, B. Nath& K. Ramamohanarao 2007	Conditional Random Fields	Using conditional Random Fields as a model in a toolkit (CRF++)	Malicious attack, denial of service attack, probing attack, R2L (unauthorized access from a remote machine) or U2R (unauthorized access to root) attack.	To use conditional Random Fields as a model in a toolkit (CRF++) for much robustness and effective result in intrusion detection.	YES	NO	Unknown attacks cannot be detected by proposed model.
Yihua Liao & V. RaoVemuri 2002	Text categorization technique	Text categorization technique is used for transforming the documents and to make them representable in form of vector space model.	Malicious attack, known attacks and novel attacks	To use K-Nearest Neighbor (K-NN) algorithm in text categorization for anomaly based intrusion detection	YES	YES	Process table attack, port based attacks.
C. Kruegel, F. Valeur, G. Vigna& R. Kemmerer 2002	Stateful Intrusion technique	A technique to divide the traffic in small chunks and to thoroughly scan for intrusion detection on LINUX based environment	Multistep attacks & misuse Malicious attack	To divide the traffic in smaller portions and to thoroughly analyzed for intrusion detection for Gigabit Ethernet (1000 Mbps)	YES	YES	Very complex requirement, complex installation and dependency issue.

D.Md. Farid, N. H. Hoa, J. Darmont, N. Harbi& M. ZahidurRahman 2010	adaptive naive Bayesian tree (NBTree)	An algorithm for anomaly based intrusion detection and implemented on naive Bayesian tree	Denial of service attack, user to root attack, remote to user attack and probing attack	A new learning algorithm to be apply (NBTree) for anomaly based intrusion detection of large volume of audit data	YES	NO	Masquerader attack, port based attack, unknown attacks, results are wrong.
R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang & S. Zhou 2002	Specification-based Anomaly Detection	A technique for anomaly based intrusion detection by capturing the information from network protocols and packets for auditing the information about statics that need to be maintain to detect anomalous intrusions	External break attack, masquerader attack, penetration attack, leakage, denial of Service attack & malicious use attack	Using external finite automation for capturing the transactions on network protocols and packets for anomaly based intrusion detection	YES	YES	Complex mechanism.
M. Kumar, Dr. M. Hanumanthappa & Dr. T. V. Suresh Kumar 2011	False Positive Alert Reduction Technique	A technique for false positive alert reduction on (SNORT) open source network intrusion prevention and detection system	Spoofing attack, malicious use attack, known & unknown attacks	To review the configurations and update the security patches for reducing the false positive security alert	YES	YES	Newly born unknown attacks can never be detected by proposed solution

4. Conclusion and Future Work

Computer Networks and internet is an essential need, we have concluded that preceding environment of computer network needs more specific consideration for port injections and unknown attacks. It is negotiated above different techniques with their merits and demerits according to the nature of the practice.

The future work will be based on network ports and analyzing of suspicious traffic on port basis; as it is the very elementary source for hackers to target the victim's machine, so the future work will be focus on ports based algorithm. An algorithm would be proposed for ports based attacks and unknown attacks. Current techniques provide security for known attacks in a dedicated network environment; future work will be contributed to standalone machines for further betterment and towards achievements.

References

[1] J. M. E Tapiador , J. E. Diaz Verdejo, "Detection of Web-Based Attacks through Markovian Protocol Parsing", *Proceedings of the 10th IEEE Symposium on Computers and Communications*, page 457-462, June 2005.

[2] F.Ullah and W. Tariq, "Operating System Based Analysis of Security Tools for Detecting Suspicious Events in Network Traffic", International Journal of Computer Science Issues(IJCSI), Vol. 8, Issue 6, No 2, page 418-422 November 2011.

[3] G. Wang, J. Hao, J. Ma and L.Huang, " A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering", Elsevier's journal of Expert Systems with Applications, Volume 37, Issue 9, page 6225-6232, September 2010.

[4] Mohammad M. Rasheed, O. Ghazali, N. MdNorwawi and Mohammed M. Kadhum," A Traffic Signature-based Algorithm for Detecting Scanning Internet Worms", International Journal of Communication Networks and

Information Security (IJCNIS), Vol. 1, No. 3, page 24- 30, December 2009.

[5] T.Grandison and EvimariaTerzi, "Intrusion Detection Technology", IBM Almaden Research Center, page 1-7, September 7, 2007.

[6] C. Kruegel, D. Mutz, W. Robertson, and F. Valeur, “Bayesian event classification for intrusion detection”,*In Proc. of the 19th Annual Computer Security Applications Conference*, Las Veges, NV, 2003.

[7] K. K. Gupta, B. Nath, and K. Ramamohanarao“Conditional Random Fields for Intrusion Detection”,*In 21st International Conference on Advanced Information Networking and Applications Workshops*, IEEE, pages 203–208, 2007.

[8]YihuaLiao , V. RaoVemuri, “Using Text Categorization Techniques for Intrusion Detection”, *Proceedings of the 11th USENIX Security Symposium*, page 51-59, August 2002.

[9] C. Kruegel, F. Valeur, G. Vigna, and R. Kemmerer, “Stateful intrusion detection for high-speed networks” *In Proceeding of the IEEE Symposium on Research on Security and Privacy*. Oakland, CA: IEEE Press,May 2002.

[10] D. Md. Farid, N.HuuHoa, J.Darmont, N.Harbi, and M. ZahidurRahman, “Scaling up Detection Rates and Reducing False Positives in Intrusion Detection using NBTree”, *In Proc. of the International Conference on Data Mining and Knowledge Engineering (ICDMKE 2010)*, page 186-190,April 2010.

[11] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang, and S. Zhou, “Specification-based anomaly detection: A new approach for detecting network intrusions”, *In Proc. 9th ACM Conf. Computer and Communication Security (CCS)*, page 265–274, 2002.

[12] M. Kumar, Dr. M. Hanumanthappa and Dr. T. V. S. Kumar, "Intrusion Detection System - False Positive Alert Reduction Technique", *Proceeding. of Second International Conference on Advances in Computer Engineering* – ACE 2011, page 1-4, Aug 2011.

[13] N. B. Amor, S. Benferhat, and Z. Elouedi, “Naive bayesvs decision trees in intrusion detection systems”, *In Proceedings of the ACM Symposium on Applied Computing*, pages 420– 424, 2004.

[14] Yang, Y,” Expert Network: Effective and efficient learning from human decisions in text categorization and retrieval”,*Proceedings of the 17th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval*, 1994.

Mr. Fasee Ullah is a lecturer in the Department of Computer Sciences, City University of Science & Information Technology - Pakistan. He has teaching as well as research experience. His specialization Areas of research are: Sensor Networks, Security, WiMAX, MANET, Cryptography and Routing Protocols. He has 10 research papers published in various reputed national and international conferences and journals. Currently he has an official reviewer of IEEE and ICCTD conferences. He received his MS (IT) from SZABIST – Pakistan.

Mr. Waqas Tariq is a student of BS (Software Engineering) at Department of Computer Science, City University of Science & Information Technology. He is an undergraduate research scholar. His research interests include Network System Security, Cryptography and Software Engineering. Currently he is working on Network Security and Software Cost Estimation.

Dr. Muhammad Arshad is Assistant Professor at City University of Science and Information Technology Peshawar. He received his PhD degree in Computer Science from Liverpool John Moores University, Liverpool UK and he has more than 8 years of experience in research and academics. He has more than 12 research publications and his area of expertise are Peer-to-Peer networks, network appliances, Quality of Service, Network Security, Web Services and Home Network.

Mr. Noor Gul is a student of PhD Electronics Engineering at Department of Electronics Engineering, International Islamic University, Islamabad. His Research Interest includes: Network Security, Information Theory and Coding, Digital Communication, Digital Signal Processing and Microelectronics designing and fabrication.