International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

A STUDY OF EFFICIENT AND INTELLIGENT INTRUSION DETECTION FOR COMPUTER NETWORK(S) SECURITY

KEERTI, DR. RAJEEV YADAV

DESIGNATION- RESEARCH SCHOLAR MONAD UNIVERSITY HAPUR
DESIGNATION= (PROFESSOR) MONAD UNIVERSITY HAPUR

ABSTRACT

There are a number of critical gaps in the cyber security industry that may be filled by the creation of a lightweight, accurate, efficient, and intelligent intrusion detection and prevention system for computer network security. Organizations are always at risk of having their computer networks compromised due to the growing complexity and frequency of cyber assaults. Developing cutting-edge intrusion detection and prevention systems is crucial since conventional security measures are sometimes inadequate to fend off new forms of attack. This research aspires to fill the void by suggesting a novel approach to dealing with the ever-evolving dangers posed by the internet. Organizations are always at risk of having their computer networks compromised due to the growing complexity and frequency of cyber assaults. Developing cutting-edge intrusion detection and prevention systems is crucial since conventional security measures are sometimes inadequate to fend off new forms of attack. This research aspires to fill the void by suggesting a novel approach to dealing with the ever-evolving dangers posed by the internet.

KEYWORDS: Intrusion Detection, Computer Network, Security, cyber security industry, computer network security.

INTRODUCTION

The fast expansion of the Internet over the last several decades may be directly attributed to the development of computers, computer networks, and network communication technologies. Threats to computer network security have developed in tandem with the meteoric rise in Internet and computer-based communication. The Internet is always under assault and new vulnerabilities are discovered every day. As a result, the security of computer networks is deteriorating. Personal, societal, governmental, and organizational activities and functions are all susceptible to disruption and influenced by these dangers. As a result, network security is becoming a vital part of today's computing infrastructures. Internal users can pose a hazard to network security via suspicious activity and malicious intent (Anderson,

1980). Protecting a network from both external and internal dangers is what network security is all about (Holm, 2012). It safeguards the network infrastructure against data loss, corruption, destruction, illegal access, and Denial of Service (DoS) assaults. While safeguards like as authentication and access control systems and safeguards against attacks on the periphery are available, they are of little use against attacks launched from inside. Therefore, a Network Intrusion Detection and Prevention System (NIDPS) is an essential tool for providing an extra layer of defense against network intrusions. Even seemingly benign network traffic may conceal malicious intent. NIDPS aids the security system by looking for suspicious activity and blocking unauthorized access.

INTRUSION DETECTION AND PREVENTION SYSTEM

Due to the exponential rise of Internet and network threats over the last several decades, network security has become more important. NIDPS has grown more important as the Internet has become more susceptible to both internal and external assault. It prevents the waste, exploitation, and abuse of IT infrastructure. "An unauthorized attempt to compromise confidentiality, integrity, and availability or to violate the security mechanisms or policies of a computer or network" is what the definition of "intrusion" says. Monitoring and analyzing network events for intrusion indicators and reporting on findings is the process known as network intrusion detection (NID). Software or hardware designed to automate the NID process is called a Network Intrusion Detection System (NIDS). According to Scarfone and Mell (2010), an Intrusion Detection and Prevention System (IDPS) is a system that both detects and attempts to prevent intrusions. James P. Anderson (1980) is credited as being the first to use the term "intrusion detection" (ID). In 1987, Dr. Dorothy Denning introduced the Intrusion Detection Expert System as the first model for ID. It served as the backbone of ID creation. Since then, several different methods for dealing with NIDPS have been developed and described in diverse literatures. Although we have come a long way, there is still plenty of room for improvement in how we identify and counteract network-based assaults.

Classifications of intrusion detection and prevention system

As can be seen in Figure 1, IDPS may be broken down into a few distinct groups depending on factors such as monitoring setting, detection method, and kind of system. IDPS may be broken down into two distinct types, depending on the setup being monitored: NIDPS and host-based IDPS. Network intrusion detection and prevention systems (NIDPS) do this by monitoring and analyzing network traffic patterns, whereas host-based intrusion detection

and prevention systems do this by monitoring and analyzing events happening at a single computer or host. Suspicious behaviors discovered during surveillance in both systems are promptly reported and the necessary precautions are taken. Misuse-based or signature-based detection, anomaly-based or behavior-based detection, and hybrid-based detection are the three main types of IDPS that may be used to determine the presence of intrusions. By comparing network traffic to predetermined patterns or the signature of past intrusions maintained in a database, a misuse-based detection technique may identify aberrant activity. This method has a high Detection Accuracy (ACC) and a low number of false positive alarms for known intrusions, but it is susceptible to novel intrusions and variations of known intrusions. The model is built around typical actions, and then anomalous ones are identified via careful monitoring for discrepancies. However, this method frequently has a high False Positive Rate (FPR), despite its ability to identify unique and "zero days" incursions. Anomaly-based detection and misuse-based detection are combined in a hybrid technique. It takes use of the strengths of several methods while eliminating their weaknesses. Since an anomaly-based technique can spot new incursions, it is the primary focus of this study.

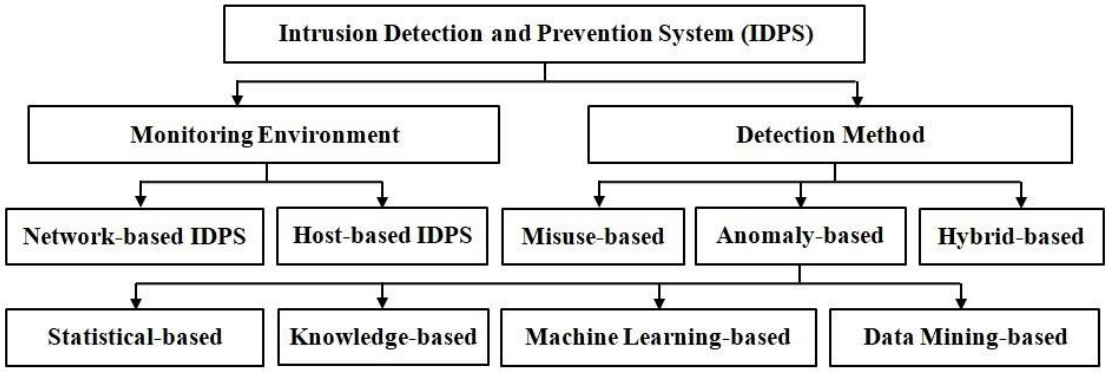

Figure 1: Classification of Intrusion Detection and Prevention System

Statistics, knowledge, machine learning, and data mining are the four primary categories of anomaly-based approaches. A statistical-based anomaly detection method uses a normal profile based on statistical attributes and tests to identify out-of-the-ordinary behavior. When it comes to detecting intrusion, a knowledge-based method that specifies the knowledge of particular attacks and vulnerabilities of network and applies this information to create warning is invaluable. The most important need for this method is maintaining an up-to-date understanding of assaults. The model that aids in classifying the observed pattern is built using a machine learning-based anomaly detection strategy. To get the best results, it builds the model in a feedback loop and adapts the execution strategy based on the data it receives.

In addition, it may pick up new skills and become better over time. The data mining-based anomaly detection method excels at "pattern finding" and may mine the big dataset for information that was previously overlooked. As a result, the quantity of redundant data used to compare network activity is decreased, which in turn generates useful data for anomaly detection. As previously mentioned, current IDS are created utilizing either anomaly based or misuse based ID models.

An intrusion detection and prevention system (IDPS) is a piece of hardware or a piece of software that may detect an intrusion and react to a detected intrusion in an effort to avert potential incidents. Each packet that enters a network is examined by an ID, which then issues an alert if an intrusion is found. It makes no attempt to stop the invasion. To stop malicious traffic from disrupting a network, administrators use intrusion prevention systems. However, IDPS can identify intrusion attempts, report them, and even block them. So it helps find intrusions early so they don't do much harm.

Intrusion Prevention System

The IDPS monitors network traffic continually and alerts the system administrator to any suspicious behavior. If you don't pair IDS with other security measures, it won't do you any good. Together, IDS and a preventive system may help stop attacks before they start and identify their origin. IDPS bogs down because of the high FAR it generates. It is suggested in how such a system may be structured, such that it is both intelligent and adaptable. The system's reaction choices might change depending on the nature of the observed occurrence. IDPS is suggested and is based on data mining. In this, we look at how to reduce false alerts by integrating numerous ID sensors. The benefits of both anomaly-based and behavior-based approaches are merged in this method. Because of these four IPS design principles, IDPS is now reliable, efficient, and applicable.

CONCLUSION

As the infrastructure of the Internet evolves, so do the opportunities for both previously unseen and previously known assaults. The network intrusion detection system (NIDS) cannot prevent all possible network intrusions. In order to build effective NIDS, there must be a detection mechanism that can identify both new and existing threats. While anomaly-based IDSs are effective at identifying both known and novel attacks, they also have a reputation for generating a large number of false alarms (both false positives and false negatives) that lower the detection ACC. The time and energy spent investigating these false

alarms may detract from the time and energy spent filtering out actual invasions. All agree that the fundamental problem for NIDS is to manage and interpret high dimensional and huge volume of class unbalanced data in real time to identify intrusion. Using this method to identify infiltration in real time is computationally expensive and time-consuming. Classifiers are crucial to NIDS effectiveness since they are responsible for real-time intrusion detection and classification. Furthermore, because classifiers require uniform misclassification costs and balanced class distribution, a dataset with an uneven number of classes makes it harder for them to accurately recognize the various forms of assault. Prediction ACC is often high for the majority class but low for the minority class in such settings. There are several intrusion detection systems available, all of which aim to improve DR and are capable of detecting various forms of assault. Surveying the research on NIDS reveals a clear preference for certain types of assaults over others, with increased ACC for some but poor or intermediate performance for others. In addition, most commercially-available NIDS do not provide network administrators with instant protection strategies after identifying certain types of attacks.

REFERENCES

Aburomman, A.A. and Reaz, M.B.I. (2016a) 'A novel SVM-kNN-PSO ensemble method for intrusion detection system', *Applied Soft Computing*, 38, 360–372. doi:10.1016/j.asoc.2015.10.011

Aburomman, A.A. and Reaz, M.B.I. (2016b) Ensemble of binary SVM classifiers based on PCA and LDA feature extraction for intrusion detection. In: *Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, IEEE, pp. 636–640. doi:10.1109/imcec.2016.7867287

Aburomman A.A. and Reaz, M.B.I. (2017) 'A novel weighted support vector machines multiclass classifier based on differential evolution for intrusion detection systems', *Information Sciences*, 414, 225–246.

Agarwal, B. and Mittal, N. (2012) Hybrid approach for detection of anomaly network traffic using data mining techniques. In: *Proceedings of 2nd International Conference on Communication, Computing and Security, Procedia Technology*, 6, pp. 996–1003.

Aghdam, M.H. and Kabiri, P. (2016) 'Feature selection for intrusion detection system using ant colony optimization', *International Journal of Network Security*, 18(3), 420–432.

Ahmad, I., Hussain, M., Alghamdi, A., and Alelaiwi, A. (2014) 'Enhancing SVM performance in intrusion detection using optimal feature subset selection based on genetic principal components', *Neural Computing and Applications*, 24(7–8), 1671–1682. doi:10.1007/s00521-013-1370-6

Ahmed, M., Mahmood, A.N., and Hu, J. (2016) 'A survey of network anomaly detection techniques', *Journal of Network and Computer Applications*, 60, 19–31.

Akashdeep, Manzoor, I., and Kumar, N. (2017) 'A feature reduced intrusion detection system using ANN classifier', *Expert Systems With Applications*, 88, 249–257.

Aljawarneh, S., Aldwairi, M., and Yassein, M.B. (2018) 'Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model', *Journal of Computational Science*, 25, 152–160. doi:10.1016/j.jocs.2017.03.006

Al-Yaseen, W.L., Othman, Z.A., and Nazri, M.Z.A. (2017) 'Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system', *Expert Systems with Applications*, 67, 296–303.

Ambusaidi, M.A., He, X., Nanda, P., and Tan, Z. (2014) 'Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm', *IEEE Transactions on Computers*, 65(10), 2986–2998. doi:10.1109/tc.2016.2519914

Amrita, and Ahmed, P. (2012) 'A study of feature selection methods in intrusion detection system: a survey', *International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)*, 2(3), 1–25.

Amrita, and Ahmed, P. (2013) A Hybrid-Based Feature Selection Approach for IDS. In: Meghanathan, N., Nagamalai, D., and Rajasekaran, S. (eds.) *Networks and Communications (NetCom2013). Lecture Notes in Electrical Engineering*, Springer, Cham, 284, pp. 195–211.

Amrita, and Ravulakollu, K.K. (2018) 'A Hybrid Intrusion Detection System: Integrating Hybrid Feature Selection Approach with Heterogeneous Ensemble of Intelligent Classifiers',

International Journal of Network Security, 20(1), 41–55. doi: 10.6633/IJNS.201801.20(1).06)
41

Amrita, Shri Kant (2019) 'Machine Learning and Feature Selection Approach for Anomaly based Intrusion Detection: A Systematic Novice Approach', *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 8(6S), 434–443.