International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

# Heuristic Approach to Intrusion Detection System

**Dr. S Brindha [1], Ms. P Abirami [2], Arjun V.[3], Logesh B. [4], Mohammed Sohail P.[5]**

[1]*HoD, Computer Networking, PSG Polytechnic College, Coimbatore Tamil Nadu India*
[2]*Professor, Computer Networking, PSG Polytechnic College, Coimbatore Tamil Nadu India*
[3,4,5]*Student, Computer Networking, PSG Polytechnic College, Coimbatore Tamil Nadu India*

---

**Abstract -** *Intrusion Detection System is used to inspect the network to identify malicious events. However, current implementation leads to significant false positives and false negatives thus making it unreliable. We propose a combination of signature and anomaly-based detection models working in tandem to identify malicious activities. This paper discuses about signature and anomaly-based IDS implementations, and proposes a hybrid IDS with signature and heuristic capabilities, which is designed to offer superior pattern analysis and anomaly detection thereby reducing administrator intervention.*

***Key Words***: Anomaly Detection, Cyber Attacks, Detection Engine, Network Security, Intrusion Detection, Malicious Traffic, Signature Detection.

## 1. INTRODUCTION

Intrusion Detection System can intelligently monitor the network traffic to detect malicious entities trying to gain access to the system. However, they have inherent limitations when implementing a single detection method which leads to false positives and false negatives; this paper proposes a combination of signature and anomaly-based models working in tandem should be implemented. This paper compares existing detection models and proposes a hybrid IDS detection engine with heuristic capabilities named SPARTAN, which is designed to offer superior pattern analysis using LCS algorithm and anomaly detection using the BOAT algorithm thereby reducing administrator intervention.

This paper explores a new method to increase detection rates during detection. We have studied existing works to explore a solution in which signature and anomaly detection are combined to design an efficient detection engine. The proposed system can analyze a program to identify its nature i.e. malicious or non-malicious.

## 2. LIMITATIONS OF SIGNATURE AND ANOMALY BASED DETECTION

### A. SIGNATURE BASED DETECTION

A Signature-based IDS uses pattern matching techniques to inspect the packet against a frequently updated database of attack signatures which might constitute an attack. It can detect existing attacks. It also conducts deep packet inspection looking for malicious patterns in the header and payload. Even though this method is effective, there are two main limitations, namely inaccurate detection of unknown attacks, and deficiencies in pattern analysis. This is due to signature-based IDS relying on pattern matching; thus variants of the attacks can have a different signature, thereby evading detection, leading to false negatives. Secondly, implementing a root-cause analysis of the intrusion is reliable as it considers the context of the attack as well as its characteristics. But, this is a time-consuming process that can take days, even months to produce results. Conversely, implementing unique-pattern analysis is quick, and simple as it involves looking for data that is unique to be an exploit, or malicious traffic, without understanding how the vulnerability works.

### B. ANOMALY BASED DETECTION

An Anomaly-based IDS has some disadvantages in the behavioral model generated during the training phase. Initially, they compare the current network activity with the baseline parameter. Then, if a deviation is observed, the administrator is alerted to a possible attack. Although this is more effective at detecting unknown attacks, a lot of time is wasted during the training phase to create a normal baseline threshold. Moreover, every single host must be individually trained which is difficult in case of a heterogeneous environment. The detection task is inaccurate as a result of false positives due to the lack of behavioral information generated in the comparison model.

Finally, this type of IDS may send alert messages asking for unnecessary administrator intervention which is often due to a lack of information of normal behavior where the IDS cannot differentiate legitimate operations from attacks; e.g. if a new program is deployed or is updated to a new version, the IDS may classify the event as abnormal.

## 3. HYBRID INTRUSION DETECTION

As discussed in the previous section, since signature and anomaly-based IDS have some limitations, combining them is necessary to harden the intrusion detection process so that the IDS is capable of detecting both known and unknown attacks, taking advantage of both signature accuracy, as well as heuristic versatility.

An IDS with heuristic capabilities and automatic signature generation is proposed. Snort is connected to an Anomaly Detection System to detect intrusions, generate rules, and update the Snort database. The Snort IDS detects known attacks using its signature detection. Then, an engine

generates FERs with different levels of thresholds to enable unknown attack detection. Hence, the FERs whose threshold either mismatches or matches to high frequencies are marked as anomalous which are then used to generate signatures and update the Snort database. Therefore, this implementation offers an efficient IDS with less administrator intervention. This method updates the database automatically every time a malicious event is detected.

## 4. PROPOSED IDS FRAMEWORK

SPARTAN primarily focuses on improving the performance of an IDS by improving detection rate, and reducing administrator intervention. It relies on a new model for distributed anomaly detection and signature generation that adapts to attacks. The approach suggested by Hwang et al is considered in generating new signatures. The core modules of SPARTAN are signature detection engine, anomaly detection engine, and signature generation engine. The management interface coordinates communication between the administrator, and the detection engines by alerting the administrator of any significant attacks. The administrator can also configure both the components with it.

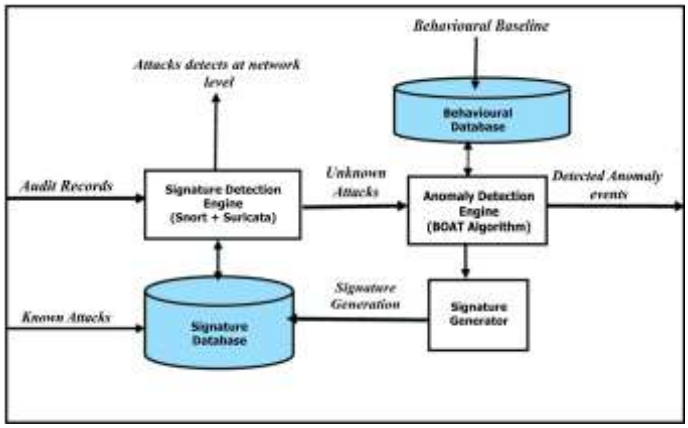


**Fig -1: HIDS Taxonomy**

A. Signature Detection Engine

The Signature Detection Engine uses pattern analysis to detect attacks. It compares the sniffed data sequences to the patterns stored in the signature database. If an attack is detected, an alert is sent to the administrator. There is very less chance of a false positive because the sequence has to match with a malicious signature before being classified as an attack. If no attack is detected, the sequence is passed onto the anomaly detection engine for further analysis in order to define whether it is abnormal behavior or not.

B. Anomaly Detection Engine

The Anomaly Detection Engine performs heuristic analysis on the sequences sent by signature detection engine. An integrated anomaly database is used to collect behavioral data so that a very accurate behavioral model can be generated. It uses boat algorithm to update the tree incrementally if the training dataset requires dynamic modifications. Each client can help to detect anomalies by defining normal behavior locally. The administrator decides whether a new event is malicious or not. If the sequence is not malicious, it is added to the database and the process continues to perform its function, otherwise the administrator is notified of the malicious event.

C. Signature Generation Engine

In order to reduce the administrator intervention due to the excessive alert messages the signature database has to be updated regularly. The proposal suggested by Hwang et al, in which the signature generation engine is part of the integrated anomaly detection engine instead of being an isolated component. SPARTAN's anomaly detection engine performs signature generation only if it detects new abnormal events. Therefore, new signatures are generated are a result of a false negatives in signature. Thus, next time the signature detection engine will detect that sequence immediately reducing both the processing time, and the administration intervention due to false positives.


**Fig -1: Management Console**

## 5. CONCLUSION

Intrusion detection should be a 360 degree defense strategy in which no single method or technology or technique should be relied upon implicitly. This paper attempts to provide an effective solution against common security threats.

**Table - 1: EXISTING MODEL VS. PROPOSED MODEL**

| PARAMETERS | EXISTING MODEL | PROPOSED MODEL |
|---|---|---|
| Correctly Classified Instances | 88.60% | 92.02% |
| Incorrectly Classified Instances | 11.39% | 7.97% |
| Mean Absolute Error | 11.4% | 10.4% |
| Root Mean Squared Error | 33.76% | 27.03% |
| Relative Absolute Error | 24.74% | 22.61% |
| True Positive Rate | 88.60% | 92.02% |
| False Positive Rate | 17.9% | 11.1% |

| | | |
|---|---|---|
| Precision | 89.1% | 92% |
| F-Measure | 88.3% | 91.9% |

One advantage of using the distributed anomaly-based IDS, in SPARTAN is the improvement in detection rate due to the consideration of heterogeneous environments. The anomaly detection model combining host and network anomaly-based detection, might increase the cost of deployment, but might significantly lower the false positives.

**ACKNOWLEDGEMENT**

We thank our HoD Dr S. Brindha and Guide Ms. P. Abirami for their guidance, expertise and encouragement. Thanks to all those who helped us in the completion of this work knowingly or unknowingly.

**REFERENCES**

[1] MAHONEY, M.V., AND CHAN, P.K. 2001. PHAD: Packet Header Anomaly Detection for Identifying Hostile Network Traffic, Florida Inst. of Technology, Florida, Melbourne, Tech. Rep. FL 32901.

[2] Martin, R.1999. Snort- Lightweight Intrusion Detection for Networks. In Proc. of 13th USENIX conference on System administration LISA '99, CA, USA, 229-238.

[3] D. Zhao, Q. Xu, and Z. Feng, "Analysis and Design for Intrusion Detection System Based on Data Mining," in Second International Workshop on Education Technology and Computer Science, Wuhan, Hubei, China, 6-7 March 2010, p. 339.

[4] Lazarevic Aleksander, Yipin Kumar, Jaideep Srivastava, Intrusion Detection: A Survey" managing cyber Threats, Springer US, pp. 19-78, 2005.

[5] Weiwei Chen, Fangang Kong, Feng Mei, Guigin Yuan, Bo Li, "a novel unsupervised anomaly detection approach for Intrusion Detection System", 2017 IEEE 3rd International Conference on big data security on cloud, May 16–18, 2017.

[6] Qingqing Zhang, Hongbian Yang, Kai Li, Qian Zhang, "Research on the intrusion detection technology with hybrid model", 2nd Conference on environmental science and information application technology IEEE, 2010.

[7] A. Jamdagni, Z. Tan, P. Nanda, X. He, and R. Liu, "Intrusion Detection Using Geometrical Structure," in Fourth International Conference on Frontier of Computer Science and Technology, Shanghai, China, 17-19 December 2009, p. 328.

[8] Ryan Trost, "Intrusion Detection Systems," in Practical Intrusion Analysis: Prevention and Detection for the Twenty First Century, Karen Gettman, Ed. Boston, USA: Addison Wesley, 2010, ch. 3, pp. 53-85.