Journal, Advances in Mathematical & Computational Sciences
Vol. 12 No. 1, 2024 Series
www.isteams.net/mathematics-computationaljournal

Journal of Advances in Mathematical & Computational Sciences
An International Pan-African Multidisciplinary Journal of the SMART Research Group
International Centre for IT & Development (ICITD) USA

Available online at https://www.isteams.net/ mathematics-computationaljournal.info
CrossREF Member Listing - https://www.crossref.org/06members/50go-live.html

Closing Disparities in Intrusion Detection: An In-Depth Analysis of IDPS Systems

Olasege I. G
Department of Computer and Electrical engineering
North Carolina Agricultural and Technical State University
Greensboro, North Carolina, United States.
E-mail: igolasege@aggies.ncat.edu.

ABSTRACT

Intrusion detection systems (IDS) are an important security tool that protects networks by monitoring policy breaches and possible threat activities Over the years, IDS technology has advanced significantly to combat cybercrime a it goes forward. The purpose of this paper is to provide a comprehensive review of IDS technology, addressing implementation challenges, research limitations, and future directions. By exploring the various research sub-categories in IDS, readers will gain insight into industry needs and the importance of ongoing research efforts

Keywords: Intrusion Detection System (IDS), Threat Detection, Attackers, Network Security, Cybersecurity Systems

AIMS-MATHS JOURNAL REFERENCE FORMAT

Olasegi, I.G. (2024): Closing Disparities in Intrusion Detection: An In-Depth Analysis of IDPS Systems. Journal of Advances in Mathematical & Computational Science. Vol. 12, No. 1. Pp 100-108. Available online at www.isteams.net/mathematics-computationaljournal. dx.doi.org/10.22624/AIMS/MATHS/V12N1P8

1. INTRODUCTION

The background of the study on Intrusion Detection and Prevention Systems (IDPS) involves understanding the fundamental concepts and principles of IDPS technologies. IDPS is defined as a system that monitors a network for possible threats to alert and prevent potential attacks [2]. It performs key functions such as detecting known attack signatures, using detection methodologies like signature-based, anomaly-based, and stateful protocol analysis, and taking preventative actions against attacks [3][5]. IDPS can be network-based or host-based, and it is closely related to both intrusion detection systems (IDS) and intrusion prevention systems (IPS) [4].

The study of IDPS is essential for enhancing network security and mitigating potential security threats. The evolution of cyber threats has been a dynamic process, influenced by technological advancements and the interconnectedness of the digital world. The historical overview of cyber threats reveals a significant shift from early viruses and simple attacks to more sophisticated and complex threats, such as zero-day attacks and ransomware. The evolution of cybersecurity can be traced back to the early days of computing when the focus was primarily on physical security, with virtual threats being a minimal risk [1].

The emergence of viruses, spyware, and more complex forms of malware marked a turning point, leading to the development of antivirus software and the recognition of the malicious potential of cyber threats [2]. Over the past decade, the world has witnessed a dramatic increase in cyber threats, with large-scale incidents such as data breaches, ransomware attacks, and global damage caused by sophisticated attacks like WannaCry and NotPetya [3]. Technological advancements have significantly impacted the complexity of cyber attacks, enabling attackers to become more sophisticated in their methods. The rise of new technologies, such as artificial intelligence, has been leveraged by cybercriminals to develop more advanced and evasive attack strategies [3]. The interconnectedness of devices and the increasing popularity of IoT (Internet of Things) have created new attack surfaces, making them prime targets for cybercriminals [3].

The evolution of cyber threats has led to the emergence of sophisticated attacks like zero-day exploits, which target previously unknown vulnerabilities, and ransomware, which can cause significant disruptions to operations and lead to financial extortion [1][4]. The year 2023 witnessed a spike in global cyberattacks, necessitating a focus on emerging security technologies such as zero trust, AI, and cloud technologies to address the evolving threat landscape [5]. The evolution of cyber threats has been characterized by a shift from simple, isolated attacks to highly sophisticated and interconnected threats, driven by technological advancements and the increasing interconnectedness of the digital world. This evolution has necessitated a corresponding focus on advanced security measures and technologies to effectively mitigate and respond to these complex threats.

The increasing vulnerability of networks and systems has underscored the need for robust security measures, including the implementation of Intrusion Detection and Prevention Systems (IDPS). IDPS plays a crucial role in proactively identifying and preventing unauthorized access and malicious activities within a network. It achieves this through a combination of passive monitoring and active blocking of suspicious or harmful network traffic. IDPS is designed to perform key functions, such as detecting known attack signatures, using detection methodologies like signature-based, anomaly-based, and stateful protocol analysis, and taking preventative actions against attacks[1][2][3]. It is closely related to both intrusion detection systems (IDS) and intrusion prevention systems (IPS), with the capability to not only detect threats but also attempt to remediate and prevent them[3]. This research aims to design, develop, and critically analyze a comprehensive IDPS that encompasses network-based, wireless, behavior analysis, and host-based security components.

Specific objectives include: The research objectives are as follows:

1. Understanding the principles and components of IDPS systems: This involves gaining a comprehensive understanding of the fundamental concepts, characteristics, and major classes of IDPS technologies [1].
2. Exploring the architecture and management of various IDPS components: It is essential to delve into the architecture, interoperability, and complementary technologies of IDPS, as well as the design, implementation, configuration, and monitoring recommendations [2].
3. Proposing a development strategy for a robust IDPS system: This entails formulating a comprehensive development strategy that encompasses network-based, wireless, behavior analysis, and host-based security components to ensure the effectiveness and coverage of the IDPS system.
4. Evaluating the effectiveness and limitations of existing IDPS systems: This involves conducting a critical analysis of the existing IDPS systems, including their benefits, drawbacks, gaps, and limitations, to identify areas for improvement.
5. Suggesting improvements and enhancements based on academic and scholarly research: The research aims to provide evidence-based suggestions and justifications for enhancing and improving IDPS systems, drawing from academic and scholarly resources to support the proposed enhancements.

2. LITERATURE REVIEW

The historical evolution of IDPS technology reveals a progression from early signature-based systems to modern, multifaceted solutions. The core objectives of IDPS encompass real-time threat detection, prevention, and swift response to mitigate potential breaches [2][4]. Classifications, including network-based, host-based, and hybrid IDPS, offer diverse approaches to combat various threats. The provided search results offer a comprehensive overview of Intrusion Detection and Prevention Systems (IDPS).

The historical evolution of IDPS technology reveals a progression from early signature-based systems to modern, multifaceted solutions [1]. The core objectives of IDPS encompass real-time threat detection, prevention, and swift response to mitigate potential breaches. Classifications, including network-based, host-based, and hybrid IDPS, offer diverse approaches to combat various threats. Detection techniques within IDPS, including signature-based, anomaly-based, and heuristic-based methods, play pivotal roles in identifying threats.

The components—sensors, analyzers, central management consoles, and response modules—form the backbone of IDPS infrastructure [4]. Effective management involving configuration, regular updates, and incident response protocols ensures optimal system functionality. The principles and components of Intrusion Detection and Prevention Systems (IDPS) are essential for understanding the system's functionality and its role in enhancing cybersecurity [1]. The detection techniques within IDPS, including signature-based, anomaly-based, and heuristic-based methods, play pivotal roles in identifying threats.

The components of IDPS, such as sensors, analyzers, central management consoles, and response modules, form the backbone of the IDPS infrastructure. Effective management involving configuration, regular updates, and incident response protocols ensures the optimal functionality of the IDPS system. A review of commercial solutions such as Snort, Suricata, and Cisco Firepower reveals their strengths, weaknesses, and suitability for diverse environments.

Open-source tools like Bro/Zeek, OSSEC, and Security Onion offer cost-effective alternatives, albeit with varying levels of community support and functionality. Frameworks like MITRE ATT&CK and the NIST Cybersecurity Framework guide IDPS implementation, aligning security practices with industry standards.

Existing IDPS technologies and frameworks offer a variety of solutions to combat cyber threats. Commercial solutions such as Snort, Suricata, and Cisco Firepower, as well as open-source tools like Bro/Zeek, OSSEC, and Security Onion, cater to diverse environments with varying levels of community support and functionality. Frameworks like MITRE ATT&CK and the NIST Cybersecurity Framework guide IDPS implementation, aligning security practices with industry standards.

3. PRINCIPLES AND COMPONENTS OF INTRUSION DETECTION AND PREVENTION SYSTEMS

The core principles governing effective threat detection within IDPS encompass the use of various detection methodologies, such as signature-based, anomaly-based, and stateful protocol analysis. These methodologies enable the system to identify possible incidents, log information about them, and attempt to stop or prevent them from succeeding [2][5]. Real-time monitoring is essential for proactive threat identification, allowing the system to detect and respond to potential threats as they occur, thereby mitigating the impact of security incidents [3][4].

Proactive prevention strategies within IDPS involve the use of response mechanisms to prevent intrusions before they occur. This includes the ability of IDPS to respond to detected threats by attempting to prevent them from succeeding, using several response techniques such as stopping the attack itself, changing the security environment, or changing the attack's content [2]. The significance of response mechanisms lies in their role in thwarting potential threats, minimizing the damage caused by security incidents, and deterring individuals from violating security policies [1][3].

3.1 IDPS Architecture Overview

The typical components of an IDPS include sensors or agents, management servers, database servers, and consoles. Sensors and agents monitor and analyze activity, while management servers handle information from sensors or agents and manage them. Database servers are repositories for event information recorded by the sensors or agents, and consoles are programs that provide interfaces for IDPS users and administrators.

Journal, Advances in Mathematical & Computational Sciences
Vol. 12 No. 1, 2024 Series
www.isteams.net/mathematics-computationaljournal

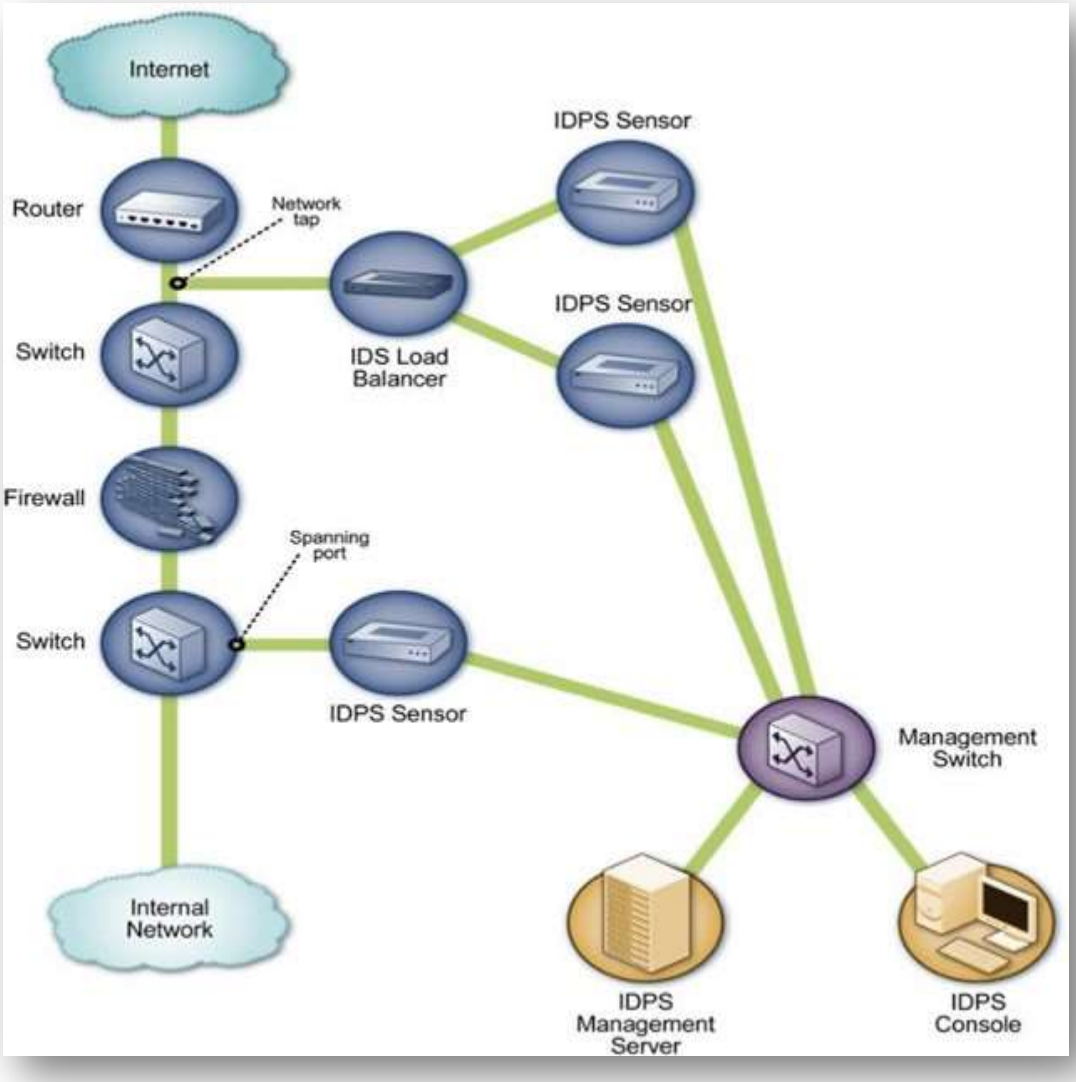

Figure 1. Inline Network-Based IDPS Sensor Architecture Example
Source: NIST SP 800-92, Guide to Computer Security Log Management, available at http://csrc.nist.gov/publications/nistpubs/

1. **Sensors or Agents**: These components monitor and analyze activity. Sensors are used to monitor networks, while agents are used to monitor hosts. Sensors capture network traffic, system logs, and other relevant data sources.
2. **Management Servers**: These servers handle information from sensors or agents and manage them. They play a crucial role in the centralized management of the IDPS infrastructure.
3. **Database Servers**: These servers serve as repositories for event information recorded by the sensors or agents. They are essential for storing and managing the data collected by the IDPS.
4. **Consoles**: Consoles are programs that provide interfaces for IDPS users and administrators. They allow for the visualization and management of the data and alerts generated by the IDPS.

3. 2 Detection Techniques

1. **Signature-Based Detection**: This method involves identifying known threats by matching patterns or signatures. It is effective in detecting known attacks but may be less effective against new or unknown threats [2].
2. **Anomaly-Based Detection**: This technique focuses on identifying deviations from normal behavior. It is effective in detecting new or unknown threats but may generate false positives [2].
3. **Heuristic-Based Detection**: This method involves identifying threats based on general rules or heuristics. It is effective in detecting new or unknown threats but may also generate false positives [2].
4. **Sensor Deployment and Functionality:** Sensors and agents monitor and analyze activity. Sensors are typically used to monitor networks, while agents are used to monitor hosts. The placement of sensors is crucial for optimal threat visibility, and they should be strategically deployed to cover critical network segments and access points[4].

3.3 Management of IDPS

The configuration process for IDPS deployment in various network architectures involves setting up the system to monitor and analyze network traffic, comparing system files, and monitoring user behavior and system patterns. The significance of tuning is to minimize false positives and optimize detection accuracy. Regular updates to IDPS signatures, rules, and databases are important to ensure the system is up to date with the latest threats. Incident response protocols are essential for handling identified threats and security incidents. Predefined response protocols are significant for swift threat mitigation. The typical components in an IDPS solution are sensors or agents, management servers, database servers, user and administrator consoles, and response modules.

These components work together to enable effective threat detection, response, and incident handling within the IDPS infrastructure. The deployment and functionality of sensors are responsible for collecting data within IDPS. The placement of sensors is crucial for optimal threat visibility, and they should be strategically deployed to cover critical network segments and access points. Analyzers process the data collected by sensors and are responsible for identifying potential threats. Accurate threat identification is essential for effective response and mitigation of security incidents. Central management consoles coordinate and manage IDPS components.

4. COMPARATIVE ANALYSIS OF IDPS COMPONENTS

A comparative evaluation of the core components constituting an Intrusion Detection and Prevention System (IDPS). The analysis delves into the effectiveness, interdependencies, and operational impact of these components within the security framework.

Table 1 – Baseline Traffic Analysis

	Baseline Traffic Analysis					
Source IP	Destination IP		Source Port	Destination Port	Bytes Transferred	
192.168.1.10	212.34.56.78		5000	80	2000	
192.168.1.20	185.76.54.32		7000	22	1500	
	Anomaly Detection					
Time	Packets Per Second					
1/15/2023 10:00	100					
1/15/2023 10:05	150					
Authentication logs indicate normal and abnormal user activities						
Time	User		Action			
1/15/2023 10:00	UserA		Login			
1/15/2023 10:05	UserB		Failed Login			
	Protocol Anomalies					
Source IP	Destination IP		Protocol	Source Port	Destination Port	
192.168.1.10	212.34.56.78		TCP	5000	80	
192.168.1.20	185.76.54.32		UDP	7000	53	
	Unusual Port Activity					
Time	Source IP		Port	Action		
1/15/2023 10:00	192.168.1.10		5000	Allow		
1/15/2023 10:05	192.168.1.20		9000	Deny		
DNS logs indicate normal and potentially malicious domain requests and Unexpected IP						
Time	Source IP	Country	Requested Domain			
1/15/2023 10:00	192.168.1.10	United Kingdom	example.co.uk			
1/15/2023 10:05	192.168.1.20	Russia	malicious-domain.com			
NetFlow data uncovers unexpected connections						
Source IP	Destination IP	Source Port	Destination Port	Protocol		
192.168.1.10	212.34.56.78	5000	80	TCP		
192.168.1.20	185.76.54.32	700	50	TCP		

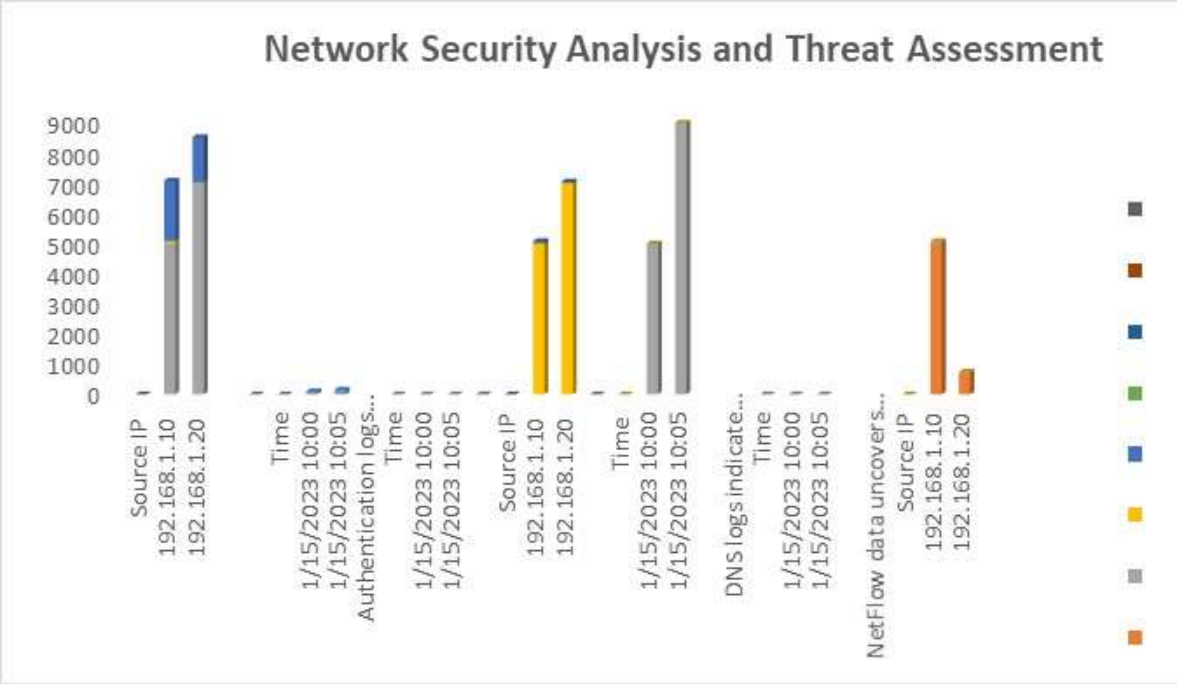

Figure 2: Network security Analysis and Threat Assessment

In this comprehensive network security analysis, an exhaustive examination of the network's activities has been performed, employing a multi-faceted approach that includes detailed baseline traffic analysis and the scrutiny of various data sources. The goal was to uncover anomalies, potential protocol irregularities, unusual port activities, and unexpected connections, thereby providing a holistic view of the network's security landscape

5. SUMMARY OF FINDINGS

1. Comparative analysis of IDPS components revealed that signature-based detection has a high detection rate but may generate false positives, while anomaly-based and heuristic-based detection are more effective in identifying emerging threats but may generate false positives. Sensors, analyzers, and response modules complement each other by providing a mechanism for monitoring, processing, and responding to potential threats. A centralized management console can improve the overall system efficacy by providing a centralized view of the IDPS infrastructure and enabling centralized management and oversight.
2. Real-world implementations of IDPS in diverse industries have shown that network-based, host-based, and wireless IDPS can be effective in detecting and preventing cyberattacks. However, there are limitations and gaps in their effectiveness, such as the challenge of reducing false positives and false negatives, the use of evasion techniques by attackers, and the legal and ethnic issues surrounding IDPS usage.

6. RECOMMENDATIONS FOR IMPROVEMENT

1. To enhance IDPS capabilities, it is recommended to integrate advanced threat intelligence, leverage machine learning for adaptive learning and behavioral analysis, and implement adaptive response mechanisms to address rapidly evolving threats. Additionally, fostering collaboration between AI systems and human experts and ensuring skilled and knowledgeable users are essential for maximizing the effectiveness of IDPS.
2. Organizations should define the requirements that the IDPS products should meet before evaluating intrusion detection and prevention products. Evaluators must understand the characteristics of the organization's system and network environments.
3. To improve IDPS efficiency and effectiveness, organizations should implement direct intrusion detection and prevention system integration, which can speed up the analysis process and help users to better prioritize threats.

REFERENCES

1. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=901146
2. https://www.rapid7.com/fundamentals/intrusion-detection-and-prevention-systems-idps/
3. https://csrc.nist.rip/library/alt-SP800-94r1-draft.pdf
4. https://www.redhat.com/en/topics/security/what-is-an-IDPS
5. https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-idps/amp/
6. https://www.redhat.com/en/topics/security/what-is-an-IDPS
7. https://csrc.nist.gov/pubs/book-section/2010/10/intrusion-detection-and-prevention-systems/final
8. https://interagencystandingcommittee.org/sites/default/files/migrated/2014-11/Annex2%20-%20Framework%20for%20Durable%20Solutions%20for%20IDPs%20%E2%80%93%20Flowcharts.pdf
9. https://nap.nationalacademies.org/read/25294/chapter/5
10. https://www.bankinfosecurity.com/5-tips-to-improve-intrusion-detection-a-4983
11. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf
12. https://ieeexplore.ieee.org/document/9817348
13.https://csrc.nist.rip/library/NIST%20SB%202007-02%20Intrusion%20Detection%20And%20Prevention%20Systems.pdf