International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

A Survey on Host-Based Intrusion Detection Systems for Endpoint Security

Asavari Virkar[1], Aarti Jadhav[2], Bhavana Gupta[3], Pradeep Shirke[4], Pranav Sawant[5]

[1,2,3,4,5]Department of Computer Engineering, Vidyalankar Polytechnic, MSBTE, Mumbai, India

Abstract

The rapid growth of cyber threats targeting endpoint devices has increased the importance of Host-Based Intrusion Detection Systems (HIDS) in modern cybersecurity architectures. Unlike Network-Based Intrusion Detection Systems, which monitor traffic at the network perimeter, HIDS focus on activities occurring directly within a host system, enabling the detection of internal attacks, malware execution, and unauthorized file access. This paper presents a comprehensive survey of Host-Based Intrusion Detection Systems, analyzing existing approaches including signature-based, anomaly-based, and hybrid detection techniques. The survey also examines key functional components such as file integrity monitoring, USB-based threat detection, encryption-based file protection, and real-time activity logging. Challenges related to resource utilization, false positives, zero-day attack detection, and usability are discussed. Finally, emerging research directions including AI-driven detection models, cloud-based threat intelligence, and automated incident response are explored to highlight future advancements in host-level security systems.

Keywords: Host-Based Intrusion Detection System, Endpoint Security, USB Malware Detection, File Integrity Monitoring, Cybersecurity, Intrusion Detection.

INTRODUCTION

The increasing dependency on digital systems and personal computing devices has significantly expanded the attack surface for cybercriminals. Modern cyber threats such as ransomware, insider attacks, USB-borne malware, and unauthorized file manipulation often target individual host machines rather than network infrastructure alone. Traditional security mechanisms, including firewalls and Network-Based Intrusion Detection Systems (NIDS), are limited in their ability to detect attacks that originate internally or bypass network monitoring layers.

Host-Based Intrusion Detection Systems (HIDS) have emerged as a critical security solution to address these challenges by monitoring system-level activities such as file access, process execution, and device interactions. By operating directly on the host, HIDS provide fine-grained visibility into system behavior and enable early detection of malicious actions. This paper surveys existing HIDS techniques, architectures, and functional components, highlighting their strengths, limitations, and applicability in securing endpoint devices against evolving cyber threats. Several studies have highlighted the importance of host-based monitoring for detecting internal and endpoint-specific attacks [2], [4], [7].

HOST-BASED INTRUSION DETECTION SYSTEM OVERVIEW

A. Core Functional Architecture

A Host-Based Intrusion Detection System operates by collecting and analyzing data generated within an individual computing system. Typical data sources include system logs, file access records, system calls, USB connection events, and user authentication activities. By correlating these events, HIDS can identify suspicious behavior that may indicate malicious intent or policy violations.

B. Role of Endpoint Monitoring

Unlike network-centric defenses, endpoint monitoring allows HIDS to detect attacks that occur entirely within the host environment. This includes privilege escalation, unauthorized file access, malware execution from removable media, and insider threats. Continuous monitoring ensures that both external and internal threats are identified promptly.

CLASSIFICATION OF HIDS TECHNIQUES

A. Signature-Based Detection

Signature-based HIDS rely on predefined patterns of known attacks, where system activities are compared against databases of malicious signatures to detect intrusions [2], [7]. This approach is efficient and generates low false-positive rates; however, it is ineffective against zero-day attacks and previously unseen threats.

B. Anomaly-Based Detection

Anomaly-based HIDS establish a baseline of normal system behavior and flag deviations as potential intrusions, enabling detection of unknown and zero-day attacks [4]. This technique is capable of detecting unknown and zero-day attacks but often suffers from higher false-positive rates due to variations in legitimate user behavior.

C. Hybrid Detection Approach

Hybrid HIDS combine signature-based and anomaly-based techniques to improve detection accuracy by leveraging the strengths of both approaches [2], [8]. Such systems reduce false positives while maintaining the ability to detect novel threats. Most modern HIDS solutions adopt this combined strategy.

KEY FUNCTIONAL COMPONENTS OF HIDS

A. File Integrity Monitoring

File integrity monitoring tracks changes to critical system files and directories, helping identify unauthorized modifications and potential malware activity [1], [5]. Unauthorized modifications, deletions, or creations are logged and flagged, helping detect malware activity, data tampering, and insider misuse.

B. USB and Removable Media Security

USB devices are a common vector for malware propagation, making removable media scanning an essential component of host-based security systems [3], [7]. HIDS solutions incorporate USB scanning mechanisms to inspect removable media before granting access, preventing the execution of malicious files and scripts.

C. Encryption-Based File Protection

To protect sensitive data, many HIDS implementations include file encryption mechanisms. Encrypted storage ensures that confidential information remains protected even if unauthorized access occurs, strengthening data confidentiality at the host level [5].

D. Logging and Alert Management

Comprehensive logging and real-time alert generation enable users and administrators to monitor system security status. Dashboards and reports provide visibility into intrusion attempts, system behavior, and historical security events.

CHALLENGES IN HOST-BASED INTRUSION DETECTION

Despite their advantages, HIDS face several challenges. Continuous monitoring can consume significant system resources, particularly on low-end devices, affecting system performance and usability [2], [4]. Anomaly-based systems may generate false positives due to dynamic user behavior, often requiring manual analysis and tuning [4], [6]. Detecting sophisticated zero-day attacks remains difficult without advanced machine learning and behavioral analysis techniques [4], [6]. Additionally, usability and platform dependency limit widespread adoption, especially in heterogeneous environments.

APPLICATIONS OF HIDS

Host-Based Intrusion Detection Systems are widely used in personal computing environments to protect against malware and unauthorized access. Educational institutions deploy HIDS in laboratories to prevent USB-based infections and monitor system misuse. Enterprises utilize HIDS for endpoint security, compliance auditing, and insider threat detection. Government and defense organizations rely on HIDS to safeguard sensitive data and critical infrastructure.

FUTURE RESEARCH DIRECTIONS

Future HIDS research focuses on integrating artificial intelligence and machine learning techniques to improve detection accuracy and reduce false positives [4], [6]. Cloud-based threat intelligence sharing can enhance real-time threat awareness by enabling continuous updates of malware signatures and behavioral profiles [2], [8]. Automated incident response mechanisms aim to isolate threats without human intervention. Expanding cross-platform compatibility and strengthening authentication mechanisms are also key areas of ongoing research.

CONCLUSION

Host-Based Intrusion Detection Systems play a vital role in modern cybersecurity by providing direct visibility into endpoint activities. This survey examined HIDS architectures, detection techniques, functional components, challenges, and applications. While existing systems offer effective protection against many threats, ongoing research is essential to address limitations related to scalability, usability, and zero-day detection. Advancements in intelligent detection and automation are expected to further strengthen host-level security in the future.

ACKNOWLEDGMENT

The authors would like to thank the Department of Computer Engineering, Vidyalankar Polytechnic, and their project guide Mr. Pradeep Shirke for his valuable guidance, continuous support, and encouragement during the preparation of this survey paper.

REFERENCES

1. “Host-Based Intrusion Detection and Prevention System (HIDPS).” ResearchGate, 2015.
2. Bridges, R.A., Glass-Vanderlan, T.R., Iannacone, M.D., Vincent, M.S., Chen, Q.

3. "A Survey of Intrusion Detection Systems Leveraging Host Data." ACM Computing Surveys, 2019.
4. Deshpande, P., Sharma, S.C., Peddoju, S.K., Junaid, S.
5. "HIDS: A Host-Based Intrusion Detection System for Cloud Computing Environment." International Journal of System Assurance Engineering and Management,
6. Vol. 9(3), 2018, pp. 567–576. DOI: 10.1007/s13198-014-0277-7
7. "A Systematic Literature Review on Host-Based Intrusion Detection Systems." IEEE Access, Vol. 12, 2024.
8. Patil, A., Dagadu, G., Aher, P.
9. "Host-Based Intrusion Detection System." IRJMETS, Vol. 6, Issue 11, November 2024.
10. Sworna, Z.T., Mousavi, Z., Babar, M.A. "NLP Methods in Host-Based Intrusion Detection Systems: A Systematic Review and Future Directions." arXiv preprint, 2022.
11. Singh, A.P., Singh, M.D. "Analysis of Host-Based and Network-Based Intrusion Detection System." International Journal of Computer Network and Information Security, Vol. 6, No. 8, 2014. DOI: 10.5815/ijcnis.2014.08.06
12. "Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges." Cybersecurity Journal, SpringerOpen, 2019.