© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716273

# Systemic Review of Intrusion Prevention Systems (IPS)

ASHIBUOGWU KEVIN[1], ESOMU SOLOMON[2], DANNY ORIARAN[3]
[1,2,3]*National Space Research and Development Agency*

***Abstract-*** ***The ever-evolving landscape of digital communications has sporadically interconnected people in various corners of the earth, ensuring optimal delivery of information. This rise in networking also led to increasing threats on network intrusion; leading to security incidents, data leaks, phishing attacks, etc. Thus, there is a need for intrusion detection and preventive systems to be actively deployed on networks for safe utilization of the numerous advantages of network systems. Intrusion detection systems when deployed actively monitors all incoming and outgoing network activities, scanning for improper network anomalies and when incongruities are detected, it sends alarms to network administrators. This type of intrusion system acts more like a passive monitoring system. An Intrusion Preventive System on the other hand, functions more as an Intrusion Detection System; however, with the added advantage that it prevents such anomalies from occurring in the first instance. This study gives an in-depth review of Intrusion Prevention Systems, detailing their various operations and how they can be deployed on active networks.***

***Index Terms-*** ***Intrusion Prevention System; Systemic Review; Network Security***

## I. INTRODUCTION

An intrusion can be defined as an unauthorized entry to other areas. In terms of computer science, it's by compromising the basic computer network security goals - confidentiality, integrity and privacy (Eom, Hong, An, Park & Kim, 2020). An intrusion prevention system (IPS) is the process of detecting intrusion malicious activities and managing responsive actions on those detected intrusions together. Intrusion prevention systems combine the best features of a firewall and Intrusion Detection System (IDS). Intrusion prevention systems (intrusion detection and prevention systems) are network security appliances that monitor network and/or system activities for malicious activity.

Intrusion Prevention System (IPS) is a technology that detects intrusion and also takes preventive actions. An Intrusion Prevention System (IPS) is a security solution that provides security against unauthorized access and malicious activities at the network level. Unlike Intrusion Detection System, that only monitors the network traffic. Intrusion Prevention System ensures protection against intrusions that take place on the network. The main function of an Intrusion Prevention System is to analyze all the inbound and outbound network traffic for suspicious activities, and perform appropriate actions instantaneously to prevent the intruders from entering into the internal network (Balamurugan, & Saravanan, 2019).

IPS offers proactive detection and prevention against unwanted network traffic, by preventing it to reach its intended victim. An IPS, when deployed correctly, immediately drops the detected unwanted or malicious data packets that may cause severe damage to the network and the resources that the network may have (Siregar, Purba, Seniman, & Fahmi, 2018). Intrusion Prevention System can be quite handy against various network security attacks such as brute force attacks, Denial of Service (DoS) attacks, vulnerability detection. Moreover, IPS also ensures prevention against protocol exploits. Intrusion Prevention System is also known as an active security solution as it does not just detect the potential security threats on the network, but it also takes immediate actions against it to prevent the current attack and the similar ones that the intruders may initiate in the future (Patil, Gunjal, Gadhe, Kulkarni, & Mandlik,2016). Intrusion prevention systems use deep network scans to pick out and cut threats and network attacks. These scans use similar attack patterns in collaboration with the activity signatures of the network to fish out malicious attempts. The system is a framework that screens network traffic for evil exercises, such as security dangers or policy compliance. It is a network security/threat prevention technology used to check the flow of network traffic to detect and prevent attacks. Vulnerability exploitation usually appears in

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716273

the form of malicious input to the target application or service. Attackers use this input to interrupt and control applications or computers. After successful exploitation, the attacker can disable the target application or potentially access all the permissions available to the infected application (Patil, Gunjal, Gadhe,

Kulkarni, & Mandlik, 2016).

Any defensive mechanism that prevents attacks before they occur is called an IPS. IPSs are IDSs that possess the same features of IDS along with the capability of preventing detected attacks (Saga & Ingle 2018). However, in the prevailing distributed environment, early prevention of attacks is impractical. The features of intrusion Prevention System (IPS) are primarily that it is a network-based defense system, with increasing global network connectivity and combines the technique firewall with that of the IDS properly with proactive technique. This system is a proactive technique that prevents attacks before entering the network by examining various data record and detects demeanor pattern recognition sensor. When an attack is identified, intrusion prevention blocks and logs the offending data. Currently, the requirement for a system to provide early detection/warning from intrusion security violation with knowledge-based has become a necessity. Therefore, the system must be active and smart in classifying and distinguishing packet data, if curious or mischievous data are detected, the alert is triggered and event response is executed (Stiawan, Shakhatreh, Kamarulnizam & Abdullahi, 2012). Figure 1 shows the features of IPS. This shows that the mechanism of prevention is activated to terminate or allow packet data to process associated with the event. It prevents attack before entering the network by examining various data records and prevents demeanor of pattern recognition.

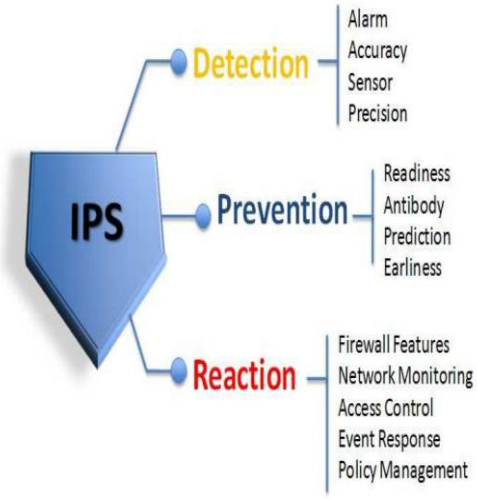


Figure 1: Feature of IPS.
(Source: Stiawan, Shakhatreh, Kamarulnizam & Abdullahi (2012))

## II. INTRUSION PREVENTION SYSTEMS AND INTRUSION DETECTION SYSTEMS

Intrusion prevention systems (IPS) are monitor real-time intrusion or which match specific profiles and will trigger the generation of alerts and it can drop, block that traffic in real-time pass through in system or network (Siregar, Purba, Seniman, & Fahmi, 2018). The main IPS focused is measures to stop an attack in progress. IPS can be termed as the new generation of intrusion detection systems (IDS) with practice to protect computers from attacks. An intrusion prevention system (IPS) is an intelligent device or software that is capable of not only monitoring malicious activities but also taking appropriate preventive actions to secure the system or the network. An intrusion detection system (IDS) is accurately suited for network attack monitoring and for alerting administrators about malicious activities (Drewek-Ossowicka, 2020). Because of its speed, performance and passive limitations has opened the door for the development of an Intrusion prevention system (IPS) to challenge it as the proactive defense choice. The key functionalities of IPS are that it detects and takes preventive actions against malicious attacks. Intrusion prevention system (IPS) stops the attack itself no more efforts are required and IPS changes the security environment (Varanasi & Razia, 2019).

Intrusion prevention system functions both as a detection system and as a prevention system. An intrusion detection system can be defined as a tool that is deployed in at the interface between the public network (interwork) and the private network to prevent the intrusion of malicious network packets(Mahrach, Mjihil & Haqiq, 2017). As the name states, the purpose of the existence of this tool is to ensure that the packets with malicious signatures should not be allowed to enter the private network as they can lead to harm if entertained. The main difference between an intrusion detection system and an intrusion detection system is that an intrusion detection system (IDS) is a monitoring system, while an intrusion prevention system (IPS) is a control system (Haider, Hu, Slay, Turnbull & Xie, 2018). An intrusion detection system (IDS) does not change network packets in any way but an intrusion prevention system (IPS) will block the transmission of data packets based on the content of the data packets, just like how a firewall prevents internet protocol (IP) addresses from communicating. On the other, the main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. In addition to that, IPS works in conjunction with an intrusion detection system (IDS) (Mahrach, Mjihil & Haqiq, 2017).

Vulnerability exploits normally come in the form of malicious inputs to an objective application or resources that the attacker uses to block and pick up control of an application or System. The role of an intrusion detection system (IDS) is to detect the malicious packet while the role to an intrusion prevention system (IPS) is to make sure that the malicious packets are being destroyed or should be blocked from execution (Seo, & Pak, 2021). The IPS works by either detecting and preventing the packets based on signature or based on the statistical anomaly. There is a sheer difference between working through both of the approaches. The detection that is being done by signature makes sure that the signature of the packets that are present in the database of the IPS will get detected while when we talk about detecting the data through statistical anomaly it checks the packet against the defined deadline. Any packet that shows any activity that has been defined under the deadline will raise the alarm and get blocked by the intrusion prevention system (IPS) (Constantinides, Shiaeles, Ghita & Kolokotronis, 2019).

Intrusion prevention systems are considered extensions of intrusion detection systems because, they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and can actively prevent/block intrusions that are detected. More specifically, an intrusion prevention system (IPS) can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address. An intrusion prevention system (IPS) can also correct Cyclic Redundancy Check errors, unregimented packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options(Fiterau-Brostean, Janssen, & Vaandrager, 2014).

The IPS must work efficiently to avoid degrading network performance. It must also work fast because exploits can happen in near real-time. The intrusion prevention system (IPS) must also detect and respond accurately, to eliminate threats and false positives (legitimate packets misread as threats) (Nakagawa, Kazato, & Nakatani, 2020). An intrusion prevention system (IPS) was originally built and released as a standalone device in the mid-2000s. This, however, was in the advent of today's implementations, which are now commonly integrated into Unified Threat Management (UTM) solutions (for small and medium-size companies) and next-generation firewalls (at the enterprise level). Intrusion prevention systems are contemplated as augmentation of Intrusion Detection Systems (IDS) because both Intrusion prevention systems (IPS) and IDS operate network traffic and system activities for malicious activity. Intrusion prevention systems (IPS) typically record information related to observed events, notify security administrators of important observed events and produce reports. Many Intrusion prevention systems (IPS) can also respond to a detected threat by attempting to prevent it from succeeding (Nakagawa, Kazato & Nakatani, 2020). They use various response techniques, which involve the Intrusion prevention system (IPS) stopping the attack itself,

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716273

changing the security environment, or changing the attack content.

| | Intrusion Detection System | Intrusion Prevention System |
|---|---|---|
| Usefulness | IDS design just only identify and examined to produce alarm | IPS design is to enhance data processing ability, intelligent, accurate of it self. |
| OSI Layer | Layer 3 | Layer 2, 3,4 and 7 |
| Signatures<br>Action | • Simple pattern matching<br>• Stateful pattern matching<br>• Protocol decode-based analysis<br>• Heuristic-based analysis | • Recognize attack pattern<br>• Blocking & response action<br>• Stateful pattern matching<br>• Protocol decode-based analysis<br>• Heuristic-based analysis |
| Activity | • A passive security solution<br>• Detect attack only after they have entered the network, and do nothing to stop attacks only just attacks traffic and send alert to trigger. | • Reactive response security solution<br>• Early Detection, proactive technique, early prevent the attack, when an attack is identified then blocks the offending data |
| Component | • Cannot expect to detect all malicious activity at all time<br>• Handling alert to trigger false positive or false negative alarm | • Can be detect new signatures or behavior attack<br>• Handling alert to trigger false positive or false negative alarm |
| Blocking future traffic | Cannot integrated with filtering rules security to stop traffic from attacking | Have the capability to block and can apply policy at perimeter router or firewall |
| Event Response | Capability only to recognize and report to security operator in the event of attack. | • Have mechanism allow, block, log, and report<br>• Integrated mechanism threat management to security operator |
| Sensor | • Commonly collected in source sensors<br>• Multisensory architectures | • Enable to integrated with other platform<br>• Have the ability to integrate with heterogeneous sensor |

Figure 2: Comparisons between IDS and IPS. Source: Stiawan, Shakhatreh, Kamarulnizam & Abdullahi (2012)

## III. SIGNATURE-BASED DETECTION

The Signature-based detection monitors the data packets in the network and compares it with a predetermined attack pattern. Signature-based detection is based on a dictionary of uniquely identifiable patterns (or signatures) in the code of each exploit. The signature is a pattern that corresponds to a known threat. In signature-based detection, observed events are compared against the pre-defined signatures in order to identify possible unwanted traffic. This type of detection technique is very fast and easy to configure (Patil, Gunjal, Gadhe, Kulkarni & Mandlik, 2016). Signature-based detection is very effective at detecting known threats but largely ineffective at detecting previously unknown threats, threats disguised by the use of evasion techniques, and many variants of known threats. An attacker can slightly modify an attack to render it undetectable by a signature-based intrusion detection system (IDS). Still, intrusion detection system (IDS) using a signature-based methodology, though having the limited capability, can be very accurate. As an exploit is discovered, its signature is recorded and stored in a continuously growing dictionary of signatures.

They have a database of signatures of all the known viruses and worms and they try to match these signatures in any file they find doubtful of infection (Yassin, Udzir, Abdullah, Abdullah, Zulzalilb & Muda, 2014). The advantage of anomaly detection is that the probability of false alarms is extremely low. It is a perfect detection of the known viruses and worms. The disadvantage of the methods is that detection of new viruses or worms is not possible. More so it cannot detect any viral activity which is not present in the file system.

Exploit-facing signatures identify individual exploits by triggering the unique patterns of a particular exploit attempt. The IPS can identify specific exploits by finding a match with an exploit-facing signature in the traffic stream. Vulnerability-facing signatures are broader signatures that target the underlying vulnerability in the system that is being targeted. These signatures allow networks to be protected from variants of an exploit that may not have been directly observed in the wild, but also raise the risk of false positives (Bakken, Orlandić & Johansen, 2019)

### Statistical anomaly detection

Statistical anomaly detection takes samples of network traffic at random and compares them to a pre-calculated baseline performance level. When the sample of network traffic activity is outside the parameters of baseline performance, the IPS takes action to handle the situation (Ray, McEvoy, Aaron, Hickman, & Wright, 2018).

### Stateful Protocol Analysis Detection

The stateful protocol analysis detection method compares the observed events with a predetermined activity profile of normal activity to identify protocol deviations. Statistical anomaly-based detection will monitor network traffic and compare it with expected traffic patterns (Huang & Feng, 2008).

## IV. NETWORK-BASED INTRUSION PREVENTION SYSTEM

Network-based IDS Notice network traffic for a special network segment and analyzes the network and software protocol activity to detect suspicious activity (Casas & Owezarski, 2012). It is most specially denoted at a boundary between networks such as in routers, firewalls, virtual private networks, etc. The main disadvantage of this type of intrusion Detection System is that it has a single point of failure. Moreover, it is weak against Denial of Service attacks. It monitors the whole network and is denoted at the boundary of the network. But it is not suitable for securing each of the hosts within the network. If an intruder can bypass it, all the systems within the network would be in trouble (Kopelo, Dhruwajita, & Jayanta, 2013). This can be considered as the other kind of IPS that is deployed in the network to prevent malicious activities. The purpose of this IPS is to monitor or keep a check on the entire network. Any malicious activity detected in the entire network can be prevented by using this kind of Intrusion prevention system (IPS). A network-based intrusion prevention system (NIPS) can be used to analyze protocol activity throughout the network to find any unreliable traffic (Kim & Park, 2003).

### Network Behavior Analysis

As the name states, this kind of IPS is used to understand the behavior of the network and all the network moving throughout the network remains in sustain surveillance of this system. Anytime the system detects the packets with malicious signature, the Intrusion prevention system (IPS) makes sure to block the packet so that it could not lead to harm to the application (Shabtai, Tenenboim-Chekina, Mimran, Rokach, Shapira & Elovici, 2014).

The main purpose of this kind of Intrusion prevention system (IPS) is to ensure that no malicious packets can be drafted and transmitted through the internal network. The organizations using this type of Intrusion prevention system (IPS) always remain protected against attacks like DOS (Denial of Service) or any kind of privacy violation-based attack(Fares, Filho, Giozza, Canedo, Mendonça, & Nze, 2019). The artificial intelligence-based platforms allow the administrators to ensure malicious activities very efficiently that are occurring in the network. All the Intrusion prevention system (IPS) has to be deployed as per their type. For instance, the host-based Intrusion prevention system (IPS) should only be deployed in a single system while the network-based IPS works fine for the entire network. All the other tools that are used to protect the network against attacks can be integrated with this system so that it could monitor the network more effectively. More specifically, the tools that scan the network or endorse the network scanning should have to be integrated with this system to enhance its performance. While other network security software is designed to detect specific endpoint intrusion, NBA tools listen to IP traffic flow systems or network packets to establish a baseline of normal activity, and then look for network flow anomalies (Akbar, Rao, & Hussain, 2016). This enables security and network managers to be alerted of any suspicious activity which is outside of normal traffic flow so that remedial action can be taken before any significant damage is done.

A network behavior analysis intrusion prevention system (NBA-IPS) is used to check network traffic to identify threats that generate strange traffic. This system can be integrated with other network scanning tools like Nexpose and so on. As the outcome, the vulnerabilities detected by those tools will also be considered by this kind of IPS and if any attack is encountered against the vulnerabilities that are witnesses by the network scanning tool, in that case, this Intrusion prevention system (IPS) will defend the system even if the patch for that vulnerability is not available.

### Host-Based Intrusion Prevention System

It can be defined as the type of intrusion prevention system which operates on a single host. In Host-based IDS (HIDS) technology, software engineers are installed on each of the computer hosts of the network to monitor the events occurring within that host only. HIDS notices network traffic and system-specific settings such as software calls, local security policy, and local log audits (Ribeiro, Saghezchi, Mantas, Rodriguez, & Abd-Alhameed, 2020). It performs log notice, file integrity checking, policy

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716273

monitoring, root kit detection, real-time alerting and active reply. HIDS are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive data. HIDS minimizes the problems incurred in Network-based IDS technology of securing special hosts in the network. But they cause a substantial overhead for the hosts running them

The purpose of this kind of Intrusion prevention system (IPS) to make sure that no malicious activity should happen in the internal network. Whenever the IPS detects any activity internally that has an abnormal signature, the Intrusion prevention system (IPS) scans the network to get more details about the activity and this way it prevents any malicious activity from happening in that particular host(Pratama, Suwastika, & Nugroho, 2018). The main feature of this kind of IPS is, it never takes care of the entire network but the single host in which it is deployed, and it keeps it very secure and entirely protected from all the attacks that could happen through the network layer.

Table 1 Comparison of IDS technology types based on their positioning within the computer system

| Technology | Advantages | Disadvantages | Data source |
|---|---|---|---|
| HIDS | • HIDS can check end-to-end encrypted communications behaviour.<br>• No extra hardware required.<br>• Detects intrusions by checking hosts file system, system calls or network events.<br>• Every packet is reassembled<br>• Looks at the entire item, not streams only | • Delays in reporting attacks<br>• Consumes host resources<br>• Needs to be installed on each host.<br>• It can monitor attacks only on the machine where it is installed. | • Audits records, log files, Application Program Interface (API), rule patterns, system calls. |
| NIDS | •Detects attacks by checking network packets.<br>•Not required to install on each host. •Can check various hosts at the same period.<br>•Capable of detecting the broadest ranges of network protocols | •Challenge is to identify attacks from encrypted traffic. •Dedicated hardware is required.<br>•It supports only identification of network attacks. •Difficult to analysis high-speed network. •The most serious threat is the insider attack. | •Simple Network Management Protocol (SNMP)<br>•Network packets (TCP/UDP/ICMP),<br>•Management Information Base (MIB)<br>•Router NetFlow records |

Wireless Intrusion Prevention System

It is considered as the other type of intrusion detection system that operates over the wireless network. This kind of Intrusion prevention system (IPS) is deployed to monitor malicious activity in the wireless network. All the packets moving within the wireless network are being checked or monitored by this kind of Intrusion prevention system (IPS) with the help of signatures (Choi, Hwang & Choi, 2017).

A wireless local area network Intrusion Detection System is similar to Network IDS in that it can examine network traffic. However, it will also examine wireless-specific traffic, including analysis for external users trying to connect to access point (AP), rogue APs, users outside the physical area of the company, and WLAN IDSs built into APs. As networks more and more support wireless technologies at various points of a topology, WLAN IDS will play huge roles in security. Many back

NIDS tools will include improvements to support wireless traffic analysis (Pund, & Athawale, 2017).

The primary purpose of a WIPS is to prevent unauthorized network access to local area networks and other information assets by wireless devices. These systems are typically implemented as an overlay to an existing Wireless LAN infrastructure, although they may be deployed standalone to enforce no-wireless policies within an organization. Some advanced wireless infrastructure has integrated WIPS capabilities (Athawale, 2017). Large organizations with many employees are particularly vulnerable to security breaches caused by rogue access points. If an employee (trusted entity) in a location brings in an easily available wireless router, the entire network can be exposed to anyone within range of the signals. If any packet is found, for which the Intrusion prevention system (IPS) has the mark of malicious signature, the IPS will prevent the packet from entering further in the network. It is one of the optimal kinds of IPS as these days wireless networks are used more often rather than the LAN-based network. It makes the network ample secure and prevents the entire harmful network packet to make any change in the existing environment (Fares, Filho, Giozza, Canedo, Mendonça, & Nze, 2019).

In computing, a wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention). The primary purpose of a WIPS is to prevent unauthorized network access to local area networks and other information assets by wireless devices (Kim, Xun, & Jung, 2016). These systems are typically implemented as an overlay to an existing Wireless LAN infrastructure, although they may be deployed standalone to enforce no-wireless policies within an organization. Some advanced wireless infrastructure has integrated WIPS capabilities. Large organizations with many employees are particularly vulnerable to security breaches caused by rogue access points. If an employee (trusted entity) in a location brings in an easily available wireless router, the entire network can be exposed to anyone within range of the signals

A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools (Nada & Al-Mosa, 2018). The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices. Rogue devices can spoof MAC address of an authorized network device as their own (Anathi, & Vijayakumar, 2020). New research uses a fingerprinting approach to weed out devices with spoofed MAC addresses. The idea is to compare the unique signatures exhibited by the signals emitted by each wireless device against the known signatures of pre-authorized, known wireless devices.

A wireless intrusion prevention system (WIPS) also includes features that prevent the threat *automatically*. For automatic prevention, it is required that the WIPS can accurately detect and automatically classify a threat. The following types of threats can be prevented by a good WIPS; (Choi, Hwang, & Choi, 2017)

a) Rogue access points – WIPS should understand the difference between rogue APs and external (neighbor's) APs
b) Mis-configured AP
c) Client mis-association
d) Unauthorized association
e) Man-in-the-middle attack
f) Ad hoc networks
g) MAC spoofing
h) HoneyPot / evil twin attack
i) Denial-of-service attack

When implementing a wireless intrusion system in a network. The WIPS implementation, server, sensors and console are all placed inside a private network and are not accessible from the Internet. Sensors communicate with the server over a private network using a private port. Since the server resides on the private network, users can access the console only from within the private network (Zhang, Chen, Weng, & Wang, 2010). A network implementation is suitable for organizations where all locations are within the private network. In a hosted WIPS

implementation, sensors are installed inside a private network. However, the server is hosted in a secure data center and is accessible on the Internet. Users can access the WIPS console from anywhere on the Internet. A hosted WIPS implementation is as secure as a network implementation because the data flow is encrypted between sensors and server, as well as between server and console.

## V. APPROACHES TO INTRUSION DETECTION AND PREVENTION

One approach to IDPS is Pre-emptive Blocking that seeks to prevent intrusion from happening before they occur. The above method is done by observing any danger signs of imminent threats and then blocking a user or IP address from which these signs originate. This technique includes attempts to detect early footprinting of an imminent intrusion then blocking IP or user that is a source of foot-printing activity. If Admin finds that particular IP address is a source of frequent port scans and other scans of their system then they will block that IP address at the firewall (Asish, & Aishwarya, 2019). **I**ntrusion detection and avoidance can be quite complicated which could potentially block a legitimate user by mistake. The complexity arises from distinguishing legitimate traffic from that indicative of an impending attack. This can lead to the problem of false positives, in which the system mistakenly identifies legitimate traffic as some form of attack (Yasir, & Croock, 2020). A software system will simply alert the administrator that suspicious activity has taken place. The human admin then decides whether or not to block traffic. If software automatically blocks any addresses it deems suspicious, you run the risk of blocking out legitimate users. It should also be noted that nothing prevents an offending user from moving to different machines to continue the attack. This sort of approach should only be one part of an overall intrusion-detection strategy and not the entire strategy

### Anomaly Based Detection

Anomaly detection is a technique of detecting any deviant behavior of the computer whose behavior is being monitored by the system. Anomaly-based detection is the process of comparing definitions of what activity is considered normal against Observed events to identify significant deviations ((Yassin, Udzir, Abdullah, Abdullah, Zulzalilb & Muda, 2014). An IDS using anomaly-based detection has profiles that represent the normal behavior of such things as users, hosts, network connections, or applications. The profiles are developed by monitoring the characteristics of typical activity over a while. The major benefit of Anomaly-based detection techniques is that they can be very useful for detecting unwanted traffic that is not specifically known. For instance, anomaly-based IDS will detect that an Internet protocol (IP) packet is malformed. It does not detect that it is malformed in a specific way but indicates that it is anomalous (Latah & Toker, 2018).

### Threshold Monitoring

Threshold monitoring pre-sets acceptable behavior levels and observes whether these levels are exceeded. This could include something as simple as a finite number of failed login attempts or something as complex as monitoring the time user is connected and the amount of data the user downloads. Threshold monitoring defines acceptable behavior. Characterizing intrusive behavior only by threshold limits can be somewhat challenging. It is often quite difficult to establish proper threshold values or proper time frames at which to check those threshold values (Kebande, Karie, Wario, & Venter, 2018). This can result in a high rate of false positives in which the system misidentifies normal usage as a probable attack. Resource Profiling measures the system-wide use of resources and develops a historic usage profile. Abnormal readings can be indicative of illicit activity underway. It might be difficult to interpret the meaning of changes in overall system usages. An increase in usage might simply indicate something benign like an increased workflow rather than an attempt to breach security. The two different ways of anomaly detection are Profile Based Anomaly Detection and Signature Based Anomaly Detection.

### Profile Based Anomaly Detection

A behavior is called anomalous if it deviates significantly from the normal behavior. Therefore, for anomaly detection, the first thing that needs to be done is to learn the profile of the system. Most

precious work done in the area of anomaly detection has used the profiles for user behavior and uses this profile for matching against the system behavior (Fernandes, Rodrigues & Proença, 2015). The anomalies are detected using these profiles which are either statistical or are learned using some machine learning technique like neural networks. Another method of building a system profile as described in is by building a profile of every root level process running on the system and monitors every process for possible anomalies. The advantage of profile-based anomaly detection is that it is possible to detect new viruses and worms because this method is not dependent. It does not need any updates or patches on the advent of a new virus. In addition, it is possible to detect viruses and worms that do not reside on the file system. On the other hand, it is difficult to describe a heuristic that will work on all kind of computer systems. In addition, the probability of false alarms is high, both for false negative and false positive depending on the threshold (Fortunati, Gini, Greco, Farina, Graziano & Giompapa, 2016).

Table 2 Comparisons of intrusion detection methodologies. Source: Chang (2002)

| Detection methods | Advantages | Disadvantages |
|---|---|---|
| Signature-based intrusion detection systems (SIDS) | • Very effective in identifying intrusions with minimum false alarms (FA).<br>• Promptly identifies the intrusions.<br>• Superior for detecting the known attacks.<br>• Simple design | • Needs frequent updates with a new signature.<br>• SIDS is designed to detect attacks for known signatures. When a previous intrusion has been altered slightly to a new variant, then the system would be unable to identify this new deviation of a similar attack.<br>• Unable to detect the zero-day attack.<br>• Not suitable for detecting multi-step attacks.<br>• Little understanding of the insight of the attacks |
| The anomaly-based intrusion detection system (AIDS) | • Could be used to detect new attacks.<br>• Could be used to create intrusion signature | • AIDS cannot handle encrypted packets, so the attack can stay undetected and can present a threat.<br>• High false positive alarms.<br>• Hard to build a normal profile for a very dynamic computer system.<br>• Unclassified alerts.<br>• Needs initial training. |

## VI. GENERAL TYPES OF NETWORK SECURITY ATTACK AND INTRUSION

An intrusion in cyber security is any externally forced incident that threatens the security or function of a host, application, or network (Iradukunda & Ali, 2019). Anytime that an organization's digital infrastructure operates off-course from its normal operations, is either a glitch in the software (IT incident) or an intrusion (cyber-attack). An intrusion detection system for this type is called anomaly-based IDPS. Masquerade attacks are detected by typical behavior profiles or violations of security constraints. These intrusions are also detected using anomaly-based IDPS. Penetrations of the security control system, which are detected by monitoring for specific patterns of activity. - Leakage, which is detected by the typical use of system resources. Denial of service, which is detected by the typical use of system resources(Ge, Yue, Xie, Deng & Hu, 2018) Malicious use is detected by typical behavior profiles, violations of security constraints, or the use of special privileges. Other types of attacks are:

a) Trojan horse: A Trojan horse is a malicious program that appears to be useful and installed on a computer. Because of their innocent look, users are encouraged to press and download the software. After installing the software, a range of functions such as the stole of information, keystrokes monitoring or manipulation of data is performed in the database (Sharifi, Mohammadiasl, Havasi, & Yazdani, 2015).

b) Malware: Malware attacks are among the most serious cyber-attacks designed especially to disable or access a targeted computer system unauthorized. The most popular malware is self-replicating, i.e. it gets access via the internet while infecting a certain device and from there it contaminates all network-connected systems. An additional endpoint computer will also become infected if it is connected. It runs faster than the others (Gan, Feng, Zhang, Zhang, & Zhu, 2020).

c) Botnet: It's a private computer network that is a victim of malware. By knowing the user, the hacker controls all machines on the network. Every network machine is called a zombie because it is intended to spread, infect or lead the attacker on large numbers of computers (Koroniotis, Moustafa, Sitnikova, & Turnbull, 2019).

d) Man in the Middle: A man in the middle attack is someone standing between you and the other personal interaction. By being in the center, an intruder may easily intercept, monitor and control the communication; for example, the device in the layer may not be able to determine the receiver with which they exchange information when the lower layer of the network sends information (Song & Lee, 2016).

e) Packet Sniffer: If a passive receiver is mounted on the wireless transmitter's land, it will store copies of each transmission packet. Such packages may include confidential information, sensitive and critical information, commercial secrets, etc. It will get through it when it flies across a packet receiver. The receiver acts as a sniffer to the packet and then sniffs all the packets that are sent to the sector. Cryptography is the most effective protection against sniffers (Ogbu, & Agana, 2019).

f) IP Spoofing: This method uses a fake source address to insert packets into the Internet and is one way to masquerade them as another user. End-point authentication, which guarantees that a message from the location we have decided is certain, would help to protect against IP spoofing (Shalini, Priyadharshini, & Vinothini (2020).

g) Distributed Denial of Service: The dos attack is a complicated version and much harder to detect and protect than a dos attack. The attacker uses multiple compromised systems to target a single targeted dos attack system. In this assault, the assault from DDoS even lifts botnets. Distributed Denial of Service is the Process of continuously sending unrelated information to the targeted system by the malicious node, which causes the authorized users to stay away from the required services. (Sharafaldin, Lashkari, Hakak & Ghorbani, 2019). DDoS is major security threat. For distributed environment, the mitigation of DDoS attack is very difficult but is necessary to prevent the user and network resources from this attack Distributed Denial of Service attack are packet flooding attacks which continuously flood the victim node with irrelevant packages, which is the contrast from logical DoS attack which harms the operating system or Application. It blocks the service to the valid node by continuously flooding the service providers. The DDoS attack victims consist of the targeted nodes and the machines that are used by the attacker in the DDoS attacks. In Distributed Denial of Service attack, the victim is flooded from many different sources, around hundreds of sources (Paharia, & Bhushan, 2020).

h) Worm: Without user support, a worm will reach a computer. If a user runs a vulnerable network program, a malware attacker may send malware to that application on the same Internet connection. The application will accept and execute malware from the internet to build a worm (Rodriguez, Cheng & Doan, 2019).

i) Virus: A virus cannot run itself; the interaction between the user and the machine is needed to infect and spread across the network. An example is an email containing a malicious link or an attachment. The malicious code triggers or eliminates system security controls when a receiver opens the attachment or clicks the connection. It is inefficient. In this scenario, the user corrupts the computer inadvertently (Asish & Aishwarya, 2019).

REFERENCES

[1] Aguila-Obra, & Padilla. (2006). Organizational factors affecting technology adoption. *Internet Research, 16(1)*, 94-110.

[2] Anis, Rahman, Alam, Nabil, & Hasan. (2014). Development of electronic voting machine with the inclusion of near field communication id cards, biometric fingerprint sensor, and pos printer. *School of Engineering and Computer Science BRACU*, 1-33.

[3] Aurora. (2009, July 18). *Global Research: United State Voting Procedures.* Retrieved from Thewe: http://www.thewe.cc/contents/more/archive/united_states_voting_procedures.html

[4] Ayeni, & Esan. (2018). The impact of ICT in the conduct of elections in Nigeria. *Am J Compt Sci Inform Technol 6(1)*, 23-36.

[5] Ayo, Adebiyi, & Sofoluwe. (2012, May 8). *E-Voting Implementation in Nigeria: The Success Factors.* Retrieved from ePrint: Covenant University: http://eprints.covenantuniversity.edu.ng/id/eprint/873

[6] Delaune, Kremer, & Ryan. (2010). Verifying privacy-type properties of electronic voting protocols: A taster. *Unpublished paper. School of Computer Science, University of Birmingham*, 1-43.

[7] Ducklin. (2018, July 29). *20 years ago today! What we can learn from the CIH virus.* Retrieved from Naked Security: https://nakedsecurity.sophos.com/2018/04/26/20-years-ago-today-what-we-can-learn-from-the-cih-virus/

[8] Esan, & Ayeni. (2007). E-voting in Nigeria: Barriers to full implementation. *Journal of Computing Engineering and Technology, 7(1)*, 1-21.

[9] Gibson, Krimmer, Teague, & Pomares. (2016). A review of E-voting: the past, present, and future. *Annals of Telecommunications, 23(11)*, 279-286.

[10] Infante, Rancer, & Womack. (1997). Building communication theory. *Prospect Heights, III: Waveland Press*, 17-22.

[11] Kalaichelvi, & Chandrasekaran. (2011). Design and analysis of the secured electronic voting protocol. *Journal of Theoretical and Applied Information Technology,34(2)*, 23-46.

[12] Lipton, Sanger, & Shane. (2016, March 23). *The perfect weapon: How Russian cyber power Invaded the U.S.* Retrieved from NY Times: https://www.nytimes.com/2016/12/13/us/politics/ -hack-election-dnc.html

[13] Naveenraj, Arun, Gowtham, Laleth, Naveen, & Kumar. (2019). The biometric-based electronic voting system using Aadhar. *International Journal of Innovative Technology and Exploring Engineering (IJITEE), 8(65)*, 196-199.

[14] Norman. (2002). *The psychology of everyday things, 2nd Edition.* Illinois, USA: Northbrook.

[15] Ojo, & Ihemeje. (2019). Designing e-voting as an apparatus for combating election rigging: A Nigerian Model. *Journal of Social and Political Sciences, 2(3)*, 1–21.

[16] RifkiSuwandi, & Nasution. (2016). Okamoto-Uchiyama homomorphic encryption algorithm implementation in the E-voting system in IEEE Trans. *International Conference on Informatics and Computing (ICIC)* (pp. 2–16). Glassglow UK: IEEE.

[17] Sabo, Siti, Abdullah, & Rozita. (2015). Issue and challenges of the transition to e-voting technology in Nigeria. *Journal of public policy and administration research, 5(4)*, 23–56.

[18] Sinha, & Singh. (2015). Securing mobile phone-based voting by integrating location services with an encryption algorithm . *International Journal of Computer Trends and Technology, 23(1)*, 23-56.

[19] Uzedhe, & Okhaifoh. (2016). A technological framework for transparent E-voting solution In the Nigerian electoral system. *Nigerian Journal of Technology (NIJOTECH), 35(3)*, 627–636.

[20] Van, Freeman, Van, Mitchell, James, Galvao, . . . Spiegelhalter. (2019). Communicating uncertainty about facts, numbers, and science. *Soc. open sci.6(1)*, 81-87.

[21] Wayne. (2019, November 1). *Diffusion of innovation theory.* Retrieved from SPHWEB: https://sphweb.bumc.bu.edu/otlt/MPH-Modules/SB/BehavioralChangeTheories/BehavioralChangeTheories4.html

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716273