ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 10, October 2016

A Critique of IPS Tenors

[1] Dr.K.Prabha [2] S.Sudha Sree
[1]Assistant Professor, [2] Research Scholar,
[1][2]Department Of Computer Science,
Periyar University PG Extension Centre, Dharmapuri - 636705, INDIA

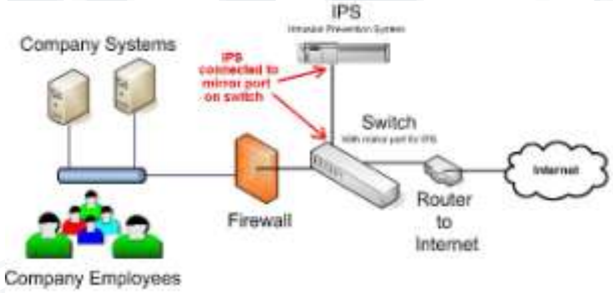
Abstract: **-- the Internet has experienced tremendous growth. Along with the widespread evolution of new emerging services, the quantity and impact of attacks have been continuously increasing. Defence system and network monitoring has become an essential component of computer security to predict and prevent attacks. Defense system and network monitoring has becomes essential component of computer security to predict and prevent attacks. Unlike traditional Intrusion Detection System (IDS), Intrusion Prevention System (IPS) has additional features to secure computer network system. In this paper, we present mapping problem and challenges of IPS. When this study was started in late 2000, there are some models and theories have been developed. Unfortunately, only a few works have done mapping the problem in IPS area, especially in hybrid mechanism.**

Index Terms— **Intrusion detection, Intrusion prevention,**

I. INTRODUCTION

The definition of IPS being used for the purposes of this paper is the ability to detect and prevent activity on or being introduced to a corporate network. There are multiple ways of providing this IPS capability and we will cover a few within this paper. In particular, we will look at the strengths and weaknesses of combining IPS and IDS technologies together. Unfortunately, most organizations that operate large internal networks are bound by the financial and man-power limitations of reality, and lack the resources, one way or another, to deploy the dozens or even hundreds of individual appliances necessary to operate an effective defense in depth strategy.

The increase in data of network traffic, involvement of human in the detection system is a non-trivial problem. IDS's ability to perform based on human expertise brings limitations to the system's capability to perform autonomously over exponentially increasing data in the network. Intrusion detection techniques based on machine learning and soft computing techniques enable autonomous packet detections. The primary difference between the two systems is that Intrusion Prevention Systems are placed in-line and are therefore able to actively prevent/block intrusions that are detected. More specifically, an IPS can take such actions as sending an alarm, dropping malicious packets, resetting the connection and/or blocking traffic from an offending IP address. An IPS can also correct Cyclic Redundancy Check (CRC) errors, defragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options.



(a).Intrusion Prevention System.

A robust IDSs system lays a foundation to build an efficient Intrusion Detection and Prevention System IDPS. Whereas the two systems often coexist, the combined term intrusion detection and prevention system (IDPS) is commonly used to describe current anti-intrusion technologies. As IDPS terminology point of view, some standard terms list as below:

- ***Alert:*** Raising an alert in the form of audible signals, email messages, page notifications or pop-up windows.

- ***Evasion:*** Changing format by an attacker to avoid from detecting by IDPS. False negative: Failure of detecting a real attack by IDPS. Whereas, the main function of IDPS is detect and respond to attacks.

- ***False attack stimulus:*** Triggering of alert by an event in the absence of an actual attack. False positive: Raising alert by IDPS in the absence of an actual attack. They tend to pervasive users to be insensitive to alerts so, they reduce their activity to real intrusion events.
- ***Noise:*** Alarm events that are accurate but do not pose significant threats to information security. Unsuccessful attacks are the most popular source of IDPS noise.

- ***Site policy:*** Configuration and policy prepared by organization for implementation of IDPS.

The IPS are always online on the network to supervise the traffic and intervene actively by limiting or deleting the traffic judged hostile by interrupting the suspected sessions or by taking other reaction measures to an attack or an intrusion. The IPS functions symmetrically to the IDS; in addition to that, they analyze the connection contexts, automates the logs analysis and suspend the suspected connections. Contrary to the classic IDS, the signature is not used to detect the attacks. Before taking action, The IDS must make a decision about an action in and appropriate time. If the action is in conformity with the rules, the permission to execute it will be granted and the action will be executed. The other prevention techniques, is a relatively new technique. It is based on the principle of integrating the heterogeneous technologies: firebreak, VPN, IDS, anti-virus, anti-Spam, etc. Although the detection portion of IDS is the most complicated, the IDS goal is to make the network more secure, and the prevention portion of the IDS must accomplish that effort. After malicious or unwanted traffic is identified, using prevention techniques can stop it. A more sophisticated approach to IPS is to reconfigure network devices (e.g., firewalls, switches, and routers) to react to the traffic. Virtual local area networks (VLAN) can be configured to quarantine traffic and limit of the Connections to other resources. The IPS allows the following functionalities [8]

- supervising the behavior of the application

- Creating rules for the application

- Issuing alerts in case of violations

- correlating of the different sensors to guarantee a better Protection against the attacks

- Understanding of the IP networks

- A mastery over the network probes and the log analysis

- defending the vital functions of the network carrying out an analysis with high velocity

II. CLASSIFICATION OF IPS AND REQUIREMENTS OF EFFECTIVE PREVENTIONS

These rules will be followed in the classification of the IPS

Reliability: The generated alerts must be justified and no intrusion to escape

Reactivity: An IDS/IPS must be capable to detect and to prevent the new types of attacks as quickly as possible. Thus, it must constantly self-update. Capacities of automatic update are so indispensable. Facility of implementation and adaptability: An IDS/IPS must be easy to function and especially to adapt to the context in which it must operate. It is useless to have an IDS/IPS giving out some alerts in less than 10 seconds if the resources necessary to a reaction are not available to act in the same constraints of time.

Performance: the setting up of an IDS/IPS must not affect the performance of the supervised systems. Besides, it is necessary to have the certainty that the IDS/IPS has the capacity to treat all the information in its disposition because in the reverse case it becomes trivial to conceal the attacks while increasing the quantity of information. These criteria must be taken into consideration while classifying an IDS/IPS, as well In-line operation - only by operating in-line can an IPS device perform true protection, discarding all suspect packets immediately and blocking the remainder of that flow Reliability and availability - should an in-line device fail, it has the potential to close a vital network path and thus, once again, cause a DoS condition.

Resilience - as mentioned above, the very minimum that an IPS device should offer in the way of High Availability is to fail open in the case of system failure

or power loss (some environments may prefer this default condition to b e "fail closed" as with a typical firewall, however - the most flexible products will allow this to be user-configurable). Active -Active stateful fail-over with cooperating in -line sensors in a fail-over group will ensure that the IPS device does not become a single point of failure in a critical network deployment.
Low latency - when a device is placed in-line, it is essential that its impact on overall network performance is minimal. Packets should be processed quickly enough such that the overall latency of the device is as close as possible to that offered by a layer 2/3 device such as a switch, and no more than a typical layer 4 device such as a firewall or load- balancer.

High performance- packet processing rates must be at the rated speed of the device under real -life traffic conditions, and the device must meet the stated performance with all signatures enabled. Headroom should be built into the performance capabilities to enable the device to handle any increases in size of signature packs that may occur over the next three years. Ideally, the detection engine should be designed in such a way that the number "signatures" (or "checks") loaded does not affect the overall performance of the device.

Unquestionable detection accuracy - it is imperative that the quality of the signatures is beyond question, since false positives can lead to a Denial of Service condition. The user MUST be able to trust that the IDS is blocking only the user selected malicious traffic. New signatures should be made available on a regular basis, and applying them should be quick (applied to all sensors in one operation via a central console) and seamless (no sensor reboot required)

Fine-grained granularity and control - fine grained granularity is required in terms of deciding exactly which malicious traffic is blocked. The ability to specify traffic to be blocked by attack, by policy, or right down to individual host level is vital. In addition, it may be necessary to only alert on suspicious traffic for further analysis and investigation

Advanced alert handling and forensic analysis capabilities - once the alerts have been raised at the sensor and passed to a central console, someone has to examine them, correlate them where necessary, investigate them, and eventually decide on an action. The capabilities offered by the console in terms of alert viewing (real time and historic) and reporting are key in determining the effectiveness of the IPS product.

An extremely low failure rate is thus very important in order to maximize uptime, and if the worst should happen, the device should provide the option to fail open or support fail-over to another sensor operating in a fail -over group (see below). In addition, to reduce downtime for signature and protocol coverage updates, an IPS must support the ability to receive these updates without requiring a device re-boot. When operating inline, sensors rebooting across the enterprise effectively translate into network downtime for the duration of the reboot.

III. TYPES OF IPS AND ITS METHODS

An intrusion prevention system is "software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents"1. IPS have the same two major categories as IDS: network-based and host-based systems

A. Network-based Intrusion Prevention Systems

Network-based IPS "perform packet sniffing and analyze network traffic to identify and stop suspicious activity"22. They add to the functions of network-based IDS with the capability to block packets that match a particular signature or behaviour23. To make this more effective, network-based IPS sit inline and act like a network firewall. They use both attack signatures and analysis of network and application protocols in comparing network activity of frequently attacked applications against expected behavior to identify suspicious activity. They are designed to detect attacks on the network before they reach their intended targets. Network-based systems are highly customizable, making it very easy for administrators to simultaneously implement attack signature for new malware threats; they can block new malware threats much before antivirus signatures become available. While network-based IPS are effective at blocking "specific known threats, such as network service worms, and e-mail borne worms and viruses with easily recognizable characteristics", they are usually incapable of stopping malicious mobile code or Trojan horses24. However, network-based IPS may be able to block some unknown threats using application protocol analysis. Stateful Signature detection – It looks at relevant portions of traffic, where the attack can be perpetrated. It does this by tracking state and based on the context specified by the user detects an attack. It is not completely automatic, as the user needs to have some prior knowledge about the attack. Protocol anomaly detection - All vendors do detailed packet analysis with protocol decode engines to ensure packets meet protocol requirements.

(b) Network based IPS

B. Host-based Intrusion Prevention Systems

Host-based IPS are similar to network-based IPS in principle and purpose, except that host-based IPS monitor the "characteristics of a single host and the events occurring within that host"25. They are also different from host-based IDS in that they can "block or reject specific applications, behaviors and changes to the local system configuration"26. Host-based IPS monitor activities such as "network traffic, system logs, running processes, file access and modification and system and application configuration changes"27.

(c) Host based IPS

C. Intrusion prevention system(IPS)

The majority of intrusion prevention systems use one of three detection methods:

- ♣ Signature-based,
- ♣ Statistical anomaly-based,
- ♣ Firewalls
- ♣ Policy based and
- ♣ Honey pot based.

1) Signature-based Detection: This method of detection makes use of signatures, which are attack patterns that can be preconfigured and predetermined. A signature-based intrusion prevention system monitors the network traffic to match with the signatures which are preconfigured and stored in a database. If a signature matches the intrusion prevention system takes the appropriate action. The signature database has to be constantly updated because of the various new attacks whose signature cannot be identified in detection.

2) Statistical Anomaly-based Detection: Anomaly detection or profile based signature monitors the network traffic that deviates from the normal traffic. A baseline is created, and the system intermittently samples network traffic, using statistical analysis to compare the sample to the already set baseline. If the activity deviates from the baseline parameters, the intrusion prevention system takes the appropriate action.

3) Firewalls: Firewalls are a form of Intrusion Prevention System. The main purpose of the firewall within the Enterprise is to enforce Enterprise policy and maintain connection state information for legitimate users internally or externally and not to prevent high volume DoS / DDoS style attacks.

4) Policy Based Detection: In a policy based detection system, a predefined set of security policies are created. Any network traffic which is detected outside the security policy will generate an alarm or drop off from the network. The policy must be designed with a detailed knowledge of the network traffic.

D. Honey-pot based System:

This uses a dummy server to attract attacks towards the network. This helps to distract attacks from real network devices. These types of systems are mainly used in production environment and large organizations which come across as targets for attackers.

(d) IPS Working in inline mode

An IPS can be defined as an in-line product that focuses on identifying and blocking malicious network activity in real time [4].IPS combines the technique firewall (data link layer, network layer, transport layer and application layer) with that of the IDS properly with proactive technique, it is a new approach system to defense networking systems and prevents attacks from entering the network by examining various data record and prevention demeanor of pattern recognition sensor. When an attack is identified, intrusion prevention blocks and logs the offending data Merits and Demerits Of the IPS working in Inline Mode.

IV. MERITS AND DEMERITS OF IPS WORKING IN INLINE MODE

Merits of IPS working in inline mode Demerits of IPS working in inline mode we can configure an IPS sensor to perform a packet drop that can stop the trigger packet, the packets in a connection, or packets from a source IP address. An IPS sensor must be inline and, therefore, IPS sensor errors or failure can have a negative effect on network traffic. Being inline, an IPS sensor can use stream normalization techniques to reduce or eliminate many of the network evasion capabilities that exist. Overrunning IPS sensor capabilities with too much traffic does negatively affect the performance of the network. Working in inline mode gives more security to the users on which the IPS is running. It can be a HIPS (Host-based Intrusion prevention system) or NIPS (Network based Intrusion Prevention system) Users deploying IPS sensor response actions must have a well thought-out security policy combined with a good operational understanding of their IPS deployments.

V. CONCLUSIONS

IPS has additional features to secure computer network system. The additional features identifying and recognizing suspicious threat trigger alarm, event notification, through responsible response. In this preliminary observation from previously researcher, hybrid techniques is one of solution for classification and detection intrusion threat. The classification rules can be used for intrusion detection (IDS) and intrusion prevention system (IPS) to classify the attack and signature.

REFERENCES

1. A Le, E. Al-shaer, and R. Boutaba, "On Optimizing Load Balancing of Intrusion Detection and Prevention Systems,"IEEE, INFOCOM Workshops, 2008.

2. A Ghorbani, W. Lu, and M. Tavallaee, "Network Intrusion Detection and Prevention," Network Intrusion Detection and Prevention,Boston, MA: Springer US, 2010, pp. 129-160.

3. Wool, "The use and usability of direction-based filtering in firewalls," Computers & Security, vol. 23, Sep. 2004, pp. 459-468.

4. Barkett, M., "Intrusion Prevention Systems", http://www.nfr.com/resource/downloads/SentivistIPS-WP.pdf

5. Ghorbani A.A, Network Intrusion Detection and Prevention : Concepts and Technique, Springer, 2009.

6. Endorf, C., Schultz, E., Mellander, J., Intrusion Detection & Prevention, McGraw-Hill 2004.

7. G. Ollmann, "Intrusion Prevention Systems (IPS) destined to replace legacy routers," Network Security, vol. 11, 2003, pp. 18-19.

8. Intrusion Detection and Prevention Scorecard [Online] Available on http://www.strategy2act.com/solutions/scorecardreports/bsc_intrusion_ prevention.html K. Alsubhi, E. Al-shaer, and R. Boutaba, "Aler Prioritization in Intrusion Detection Systems," IEEE proceeding Network Operations and Management Symposium, 2008, pp. 33-40.
9. J. Carter, E., Hogue, Intrusion Prevention Fundamentals : an introduction to network attack mitigation with Intrusion Prevention System, Cisco press, 2006.

10. KAZIENKO, Przemyslaw; DOROSZ, Piotr. Intrusion detection systems (IDS) Part 2-Classification; methods; techniques. WindowsSecurity. com, 2004.

11. "Network intrusion detection (IDS) and intrusion protection system (IPS)" [Online] Available on http://www.cdacbangalore.in/design/corporate_site/override /pdf-doc/projects/GYN.pdf.

12. Sproull, T., and Lockwood, J., "Wide-area hardware-accelerated intrusion prevention systems (WHIPS)", Proceedings of the International Working Conference on Active Networking (IWAN), Lawrence, Kansas, USA, October 27 – 29, 2004.
13. T. Dutkevych, A. Piskozub, and N. Tymoshyk, "Real-Time Intrusion Prevention and Anomaly Analyze System for Corporate Networks," IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems Technology and Application, 2007, pp. 599-602.

14. Q. Zhang and R. Janakiraman, “Indra : A Distributed Approach to Network Intrusion Detection and Prevention,” Access, vol. WUCS- 01-30, 2003, pp. 1-6.

15. W.Z. Xinyou Zhang, Chengzhong Li, “Intrusion Prevention System Design,” Computer and Information Technology, 2004. CIT ’04, 2004, pp.386-390.

16. Xinidis, K., Anagnostakis, K.G., and Markatos, E.P., “Design and implementation of a high performance network intrusion prevention system“, Proceedings of the 20th International Information Security Conference (SEC 2005), Makuhari-Messe, Chiba, Japan, May 30- June 1, 2005.