ISSN 2320 2629

Volume 1, No.2, November – December 2012
International Journal of Information Technology Infrastructure
Available Online at http://warse.org/pdfs/ijiti03122012.pdf

Multi-Tiered Architecture for Intrusion Prevention

Akhil Behl [1], Kanika Behl [2], Nikhil Behl [3]
[1] Cisco System, India, akbehl@cisco.com
[2] Jagan Institute of Management Studies, India, kanika.behl@jimsindia.org
[3] NSC Global, India, nikhilbehl@engineer.com

Abstract*:* Today with the Internet available as a general tool, access to any publicly reachable network is a way for the legit users to leverage network resources. On the other hand, it is a way for hackers and attackers to exploit a network whether it is for competitive, financial, revenge or for that matter any malicious purpose. Intrusion prevention is a key component of any security strategy in today's IT infrastructures. It adds a indispensable layer for defense in depth strategy. Firewalls or authentication systems alone are no longer sufficient to cope with modern day attacks since, firewalls only deny malicious traffic from an unauthorized source however, does not have the capability to stop malicious traffic from authorized end points/sources. Similarly, an authenticated session once compromised, can become a source of Denial of Service (DoS) attack. This paper is dedicated to research on multi-tiered Intrusion Prevention [1] architecture which can not only cope with attacks however, also ensure that the attack vector is blocked and that the attack type is realized if not already known.

Key words : Intrusion Prevention System, IPS, Network IPS, Host IPS, Multi-Tiered IPS, Security Architecture.

INTRODUCTION

Today networks are growing at a very fast pace. The Internet, which is network of networks has enabled people to connect to resources which they wish to leverage for their daily job functions, whereby providing anywhere anytime connectivity. However, at the same time, there are hackers and attackers which lurk around searching for potential targets which they can exploit for their financial benefit, as an act of revenge against their previous employer, extract information for competition purpose, or just playing role of script kiddie (casual hacking). This paper is intended to provide an overview of tiered (layered) Architecture for Intrusion Prevention Systems (IPS) [1, 2]. It examines the possibilities of placing IPS Network or Host based systems to cope with varied attacks.

The security threat landscape [3, 6] has changed drastically where organized crime makes a concerted and financially motivated effort to silently steal confidential information from specific organizations. These attacks are focused on certain key information sources and the aim is to gather all information pertinent to business or process which can benefit a competition or help improve product features by stealing information from victim organization. Ignoring traditional IT perimeter defenses [4], today hackers enter networks though connections opened by remote users, via smart phones, or hijacking instant messaging sessions. Once inside, there is minimum chance of stopping a session coming through an authorized and trusted session. Once on the inside, hackers deploy complex, stealthy crime ware methods to collect passwords, credit card information, bank account numbers, customer records, or any other type of information that they can profit from. On the other hand, an indirect way to gain monetary profit is to gather organization sensitive data [5] in terms of research, sensitive prototype, accounts, or any such data which can be sold to an organization or individual that will have drastic results for organization from which it was stolen and the acquiring organization or individual enjoys the privilege. The true goal of these attacks is to gain unauthorized access to systems and information on an ongoing basis.

When spyware or malware infects the endpoints [6], end users see their system speed and productivity grind to a slow pace. Help desks are swamped with support calls from users that can't access information or run business critical applications. Worst yet, IT administrators don't have enough time and staff to continually track down, quarantine, and repair infected endpoints. These sophisticated types of threats and attacks require new levels of protection at an organizational level barring threats originating from inside and outside. While antivirus technology can play an important role in the defense, it must be joined by a coordinated, multilayered defense that includes proactive vulnerability-based intrusion prevention, file-based intrusion prevention, and inbound and outbound traffic control.

An Intrusion Prevention System (IPS) [1, 4] has the capability of blocking offending operations. It prevents attacks by fighting them before they may cause damages to the network or hosts, rather than simply reacting to them. Attacks are answered in real time e.g. 0-day attacks. Moreover an IPS protects at the application layer level against attacks exploiting well known vulnerabilities relative to an application or an operating system. They may be tied to communication protocols such as http, ftp, TFTP etc. Such attacks use legitimate ports left open by a firewall for information exchange: for instance HTTP port (TCP 80) may be used for a web server attack behind a firewall. In such a case, the firewall will not be able to prevent the attack since, the attacker will be using legitimate ports/services and therefore, no policy can banish it. IPS [2] comes to rescue as, it can look deep into the packet structure and compare it with a known good profile/signature [3] or run through deep packet analysis to investigate [1] packet content [4]. If the offending packet is found to be malicious, it can be dropped even before it reaches the destination. This is further augmented by automatic black listing of the offending IP address/DNS name, as per security profile in IPS sensor.

As a well known fact, an IPS can utilize signature recognition, anomaly detection or file integrity checking to shun attack attempts. An IPS may be either Host IPS (HIPS) [5] which consist in specialized software components (shims) running on the host to protect or Network IPS (NIPS) [3] can be hardware device or software program sitting in-line to the network to be protected.

IPS Network sensors [12] must be inserted at the right network location [8] according to the type of protection deemed for. IPS may be either isolated components or made of several entities in a layered architecture. NIPS is explored in Fig 1.

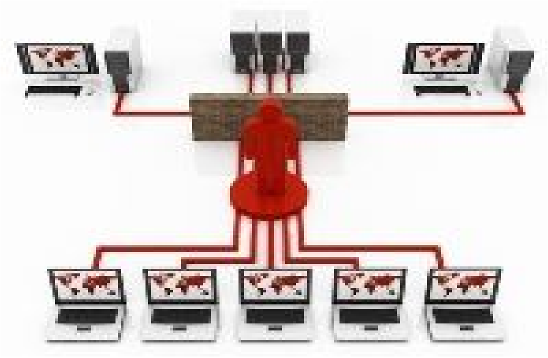


Fig 1: Network Intrusion Prevention System [10]

HIPS [11] anatomy is explored in Fig 2.

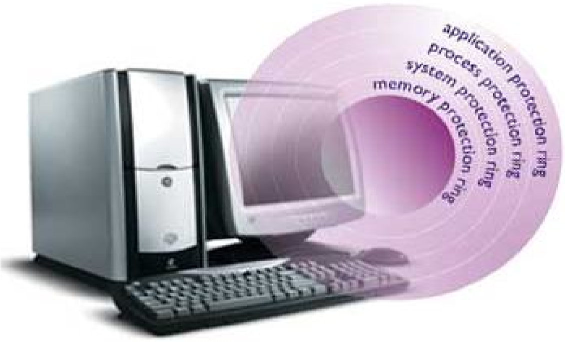


Fig 2: Host Intrusion Prevention System [11]

There are some expectations from an IPS system to be fit for consideration in a network. These considerations are as follows:

- While analyzing network traffic, it must not block normal operations however, perform blocking actions against suspicious activities [1, 4]
- It must have a high level of performance [1] and must perform accurate actions because bad attack identification will lead to a Denial Of Service (DOS)
- It must block malicious actions using signature based blocking of known attacks, as well as behavior and anomaly-based detection algorithms. These algorithms must operate at the application level in addition to standard, firewall processing [4]

In this paper we base our research on the concept of multi-tiered architecture for IPS which can thwart threats originating from within and outside an organization. This research paper is structured as follows. Section 2 explores multi-tiered architecture proposed to protect an organization’s or business’s’ internal resources from attacks originating from inside or outside. Section 3 is dedicated to analyzing benefits and shortcomings of proposed architecture and section 4 concludes the paper with research conclusion summary and next steps.

MULTI-TIERED ARCHITECTURE FOR INTRUSION PREVENTION

The efficiency of IPS based prevention relies on placement of NIPS or HIPS hardware or software based elements [2, 6] in the network. This section will examine placement strategies for IPS in a multi tiered architecture [9].

Network sensors must be inserted in the network in a way such that they can capture external or internal traffic according to the needs of an organization or as per the defined organizational security schema. They should be located preferably at traffic aggregation points to provide broader coverage. HIPS are generally installed on critical servers. An IPS sensor may be placed as shown in Fig 3.

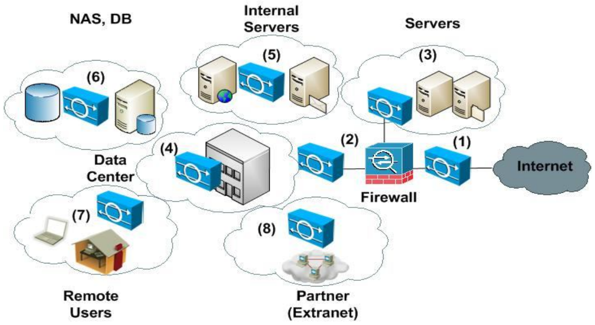


Fig 3: NIPS and HIPS Placement

1. In front of perimeter firewalls (1). It gives insight on which kind of traffic the firewalls have to cope with. In this

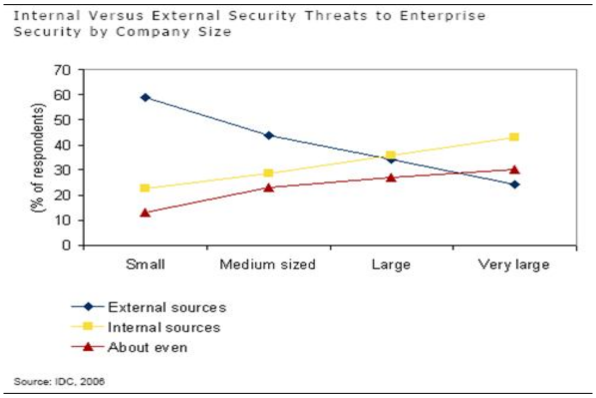
case, it must be tuned in order not to respond to attacks that the firewall will block. This tier in a multi-layer (multi-tiered) defense mechanism is very essential as it will block and shun attack/threats originating from outside resulting in lesser probability of malicious connections/software reaching internal critical systems or user systems which can be used as a hub for launching attacks on other systems, once infected.

2. Behind the firewalls that provide access to a Demilitarized Zone (DMZ) (2) or the internal network (3). A DMZ is a zone which has internet facing servers such that, even if a server is compromised in DMZ, the critical internal servers are protected on the inside zone. Behind the perimeter firewall is the most commonly used location as all traffic will pass through it. In addition to NIPS placed behind firewall, for the Internet facing servers such as Web server, DNS server, FTP server, SMTP (Mail) server etc. located in a DMZ, install a HIPS agent on each server to block server specific and directed intrusion events [3, 4]

3. On the firewall appliance itself as a module or in software running such that, all traffic passing through the firewall is inspected and suspicious packets are dropped then and there. This extends firewall’s blocking functionality.

4. At data centre or Headquarter to prevent any malicious traffic entering into main site (4) from remote sites of the organization or from remote users or vendors or partners, which leverage extranet connection to connect and access data.

5. In front of the server segments (6) or Network Area Storage devices (5) in order to protect valuable data residing on them from internal intrusion [7]. While it may sound bizarre, more often than not, most of the attacks happen from inside since, it’s easier to conduct an attack from within the organization and to conceal such an attack attempt. Figure 4 illustrates the findings from IDC research.



Internal Versus External Security Threats to Enterprise Security by Company Size

Source: IDC, 2006

Fig 4: Insider vs. Outsider attack/threat possibility

6. Behind the VPN concentrators (7), such that it may monitor the non–encrypted traffic entering from external (seemingly unsecured) network. As remote user access to the internal network is usually performed by means of VPN, this kind of traffic will be taken into account too

7. On the extranet connections (8) between the internal network and business partners where implicit trust cannot be guaranteed. The IPS will be ideally located between the business partner facilities and the shared resources

The above proposed multi tiered [9] architecture can be commonly used in almost any environment and allows having an in-depth analysis of the network security. Since, it is tiered; it means that any threat escaping one level of scrutiny can be picked up in the next level as each tier will have specific signatures or profiles for its audience (endpoints or devices).

ANALYSIS OF ADVANTAGES AND DRAWBACKS OF PROPOSED MULTI-TIERED ARCHITECTURE

In the light of proposed multi-tiered architecture for Intrusion Prevention, following are the potential advantages and drawbacks [10]:

- HIPS [5] has the ability to protect the network against internal attacks that are the most frequent [7]
- (NIPS/HIPS) IPS protects against local attacks. It prevents an attacker who has gained physical access to the system and “root” or “administrator” privileges, to compromise other systems in the network. It can shun the anomalous traffic from compromised host. It prevents attacks on systems located on the same network segment
- HIPS is useful for the protection of mobile systems once they are connected outside of the protected network e.g. on VPN
- A HIPS also protects against attacks on systems part of an encrypted network, because it analyzes the traffic once it has been decrypted
- An IPS is the “Last Line of Defense” [2] against attacks that have not been intercepted by other security tools
- A NIPS has a global view of the network due to its placement and can therefore intercept network oriented attacks [8]
- A HIPS/NIPS agent or sensor has no IP address, MAC address, nor TCP/IP stack, so it will be difficult to initiate an attack against it [4, 5]

Following are the drawbacks of the proposed model:

- A HIPS is generally closed to specific applications and operating systems and many types of HIPS may be required to protect the entire network
- A HIPS is running on the host and can be resources consuming. Moreover, as soon as the host has been compromised, a HIPS will no more be reliable [5]
- A NIPS is not able to detect attacks hidden in encrypted traffic
- A NIPS may create bottleneck in the network as all traffic has to pass through it while being analyzed in real time

CONCLUSION AND SUMMARY

While antivirus technology [6] has become the foundation for building strong client security, it is not enough. Today more than 90 percent of organizations employ some level of antivirus protection. However, even with that degree of protection, systems are still being compromised with increasing intensity. The main reason for the still-growing number of successful assaults is that antivirus solutions are reactive. They can only protect against known crime ware threats for which a remediation solution has been created. Today, professional crime ware developers focus their attacks on system and application vulnerabilities for which no specific remediation solution yet exists.

Studies [13] indicate that the average time for a vulnerability exploit to surface is six to seven days from the time that the vulnerability is discovered. A few hours after the first attack, virus definitions and signatures become available to organizations to protect themselves against these attacks. This means that organizations are typically vulnerable to new exploits for about seven days, giving full-time crime ware developers plenty of time to develop worms, bots, Trojans, or other crime ware to exploit newly announced vulnerabilities. The only way to combat against these vulnerability exploits is to employ vulnerability-based protection as part of an organization's client security solution. Instead of having to wait for a fix to a specific vulnerability, vulnerability-based protection [3] utilizes vulnerability definitions to proactively watch and protect against behavior that attempts to exploit vulnerabilities. Unlike system and application patches, a vulnerability definition can usually be created in a day or two by the security solution vendor, typically well ahead of any exploit against that vulnerability. The power of intrusion prevention comes from the fact that a single vulnerability definition is not only protecting against one type of threat, but perhaps hundreds or thousands. Since it looks for exploit characteristics and behavior, it can protect against a wide range of threats, even threats that are not yet known or developed.

An IPS system is not a colossal box like a router, performing only routing. It is rather a set of intelligent hardware [1, 2, 4, 6] (network sensors) and/or software components (shims, hosts agents) [6] which can be associated in many ways to provide a complex solution tailored to the organization security threats and business needs. Intelligence is often spread between highly specialized sensors or agents, and a centralized server, offering unique means to cope with the most pernicious attacks. A state of the art solution combines NIPS for their capacity to defend the overall network, with HIPS for their ability, by being closely linked to hosts, to put them aside of any attack.

This paper focused on developing an architecture where the rather disparate components are brought together in harmony and leveraged to provide state of art Intrusion prevention for today's networks. It goes without saying that such complete security solutions are expensive and that their architecture and deployment must be carefully studied and planned. Performance issues must not be underestimated as IPS are designed to work in line to network traffic. While there are apparent advantages to the proposed architecture, there are some hurdles [10] to be considered too. All in all, this architecture is flexible, scalable and above all universally implement able.

It is interesting future work to have the multi-tiered security architecture including intrusion prevention systems aligned with other in-line defense mechanisms which would pave path for end-to-end robust security for modern networks and can deter attacks.

REFERENCES

[1] The NSS Group. http://www.nss.co.uk

[2] CSO Online http://www.csoonline.com/article/218066/host-intrusion-prevention-is-the-last-line-of-defense-for-networks

[3] Endorf Carl, Schultz Eugene and Mellander Jim, Intrusion Detection and Prevention McGraw Hill/Osborne

[4] Lukatsky Alex. Protect Your Information with Intrusion Detection. Wayne

[5] Cisco Systems Securing Hosts using Cisco Security Agent (HIPS) http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_qanda_item09186a008049ad72.shtml

[6] Noonan Wesley J. Hardening Network Infrastructure: Bulletproof Your Systems Before You Are Hacked! McGraw-Hill/Osborne

[7] True or False: 70% of security incidents are due to insider threats? http://sbin.cn/blog/2009/11/10/true-or-false-70-of-security-incidents-are-due-to-insider-threats/

[8] Intrusion Prevention system http://en.wikipedia.org/wiki/Intrusion_prevention_system

[9] Intrusion defense – Layered plan http://www.brighthub.com/computing/smb-security/articles/2759/p3/

[10] IPS Advantages and Drawbacks http://pl.safensoft.com/security.phtml?c=587

[11] Host Intrusion prevention System http://www.securityarchitects.com/products.html

[12] Network Intrusion prevention System https://www.nsslabs.com/research/network-security/network-ips/

[13] Endpoint Security: Anti-Virus Alone is Not Enough http://www.mcafee.com/us/resources/reports/rp-aberdeen-endpoint-security.pdf