STRATEGIC SENSOR PLACEMENT FOR INTRUSION DETECTION IN NETWORK-BASED IDS

[1]Lawal, B.O. [2]Ibitola, A & [3]Longe, O. Babatope
Computer Science Department,
[1]Olabisi Onabanjo University Consult Ibadan Centre, Ibadan, Nigeria.
[2]Lead City University, Ibadan, Nigeria
[3]University of Ibadan, Ibadan, Nigeria
lawal5@yahoo.com, ibitolaayobami@yahoo.com, longeolumide@fulbrightmail.org

ABSTRACT
Network Intrusion Detection Systems (NIDSs) can be composed of a potentially large number of sensors, which monitor the traffic flowing in the network. Deciding where sensors should be placed and what information they need in order to detect the desired attacks can be a demanding task for network administrators, one that should be made as automatic as possible. Some few works have been done on positioning sensors using attack graph analysis, formal logic-based approach and Network Similator NS2 which were studied to determine a strategy for sensors placement on the network. This paper analysed the major considerations for sensors placements, typical sensors deployments in NIDS, and established an extended model for sensors deployment to further strengthen the network for intrusion detection which was based on the escape of some malicious activities through the firewall.

Index Terms– Sensors, Placement, Intrusion detection system, Network-Based IDPS.

1. INTRODUCTION

A network-based intrusion detection system (NIDS) monitors traffic at selected points on a network or interconnected set of networks. The NIDS examines the traffic packet by packet in real time, or close to real time, to attempt to detect intrusion patterns. The NIDS may examine network-, transport- and/or application-level protocol activity. Note the contrast with a host-based IDS; a NIDS examines packet traffic directed toward potentially vulnerable computer systems on a network. A host-based system examines user and software activity on a host [1].

A typical NIDS facility includes a number of sensors to monitor packet traffic, one or more servers for NIDS management functions, and one or more management consoles for the human interface. The analysis of traffic patterns to detect intrusions may be done at the sensor, at the management server, or some combination of the two [1].

One of the intrusion detection and protection system (IDPS) technologies considered to be effective in protecting organisation's network is the Sensor or Agent [2]. Sensors and agents monitor and analyze activities. The term *sensor* is typically used for IDPSs that monitor networks, including network-based, wireless, and network behaviour analysis technologies. The term *agent* is typically used for host-based IDPS technologies [2].

Effective intrusion detection for almost any large network will require multiple sensors [3]. However determining where to place a set of sensors to create cost effective intrusion detection is a difficult task. There may be several evaluation criteria for placements, seeking to maximise various desirable properties (e.g. various attack detection rates), whilst seeking to reduce undesirable properties (such as false alarm rates as well as purchase, management and communications costs). H.Chen [3] further explained that subtle tradeoffs may need to be made between the properties; different placements may have complementary strengths and weaknesses, with neither placement being uniformly better than the other.

The optimal placement of sensors depends on what is wished to achieve [3]. A placement may be optimal for the detection of one type of attack, but not for a second type of attack. We may seek a placement that gives good chances for detecting each of several types of attacks; this may yield a different optimal placement. [4].

The organization of the paper is as follows. In Section 2, review of prior research on topics related to sensor deployment in NIDS was presented. Section 3 is the necessary considerations for sensors deployment. In section 4, sensors placement in NIDS was described. Section 5 is the systems and network to watch out for. In section 6, the importance of securing the sensors was presented. Section 7 is some of the problems encountered during sensors deployment. In section 8, the extended model of sensors placement in network-based intrusion detection and prevention system was presented. Section 9 is the conclusion.

2. RELATED WORKS

Noel and Jajodia [6] propose to use attack graph analysis to find out optimal placement of IDS sensors. Attack graphs represent a series of possible paths taken by potential intruders to attack a given asset. Such graphs are constructed in a topological fashion taking into account both vulnerable services that allow nodes to be exploited and used as launch pads, and protective measures deployed to restrict connectivity. The purpose is to enumerate all paths leading to given assets and where optimal placement is devised to monitor all paths using minimal number of sensors [6]. This is seen as a set cover problem: each node allows for monitoring of certain graph edges and the challenge is to find a minimum set of routers that cover all edges in the graph; a greedy algorithm is then used to compute optimal placement.

The use of attack graphs provides an efficient mapping of network vulnerabilities in the network. A vulnerability-driven approach to deploying sensors overlooks factors such as traffic load however. As a result the placement is optimised such that the more paths that go through a node the more likely it is chosen for placement [5].

Rolando [5] introduces a formal logic-based approach to describe networks, and automatically analyse them to generate signatures for attack traffic and determine placement of sensors to detect such signatures. Their notation to model networks is simple yet expressive to specify network nodes and interconnecting links in relevant detail. While there are advantages to using a formal model, such an approach may not be scalable. The formal notation allows for a more coarse-grained specification but it is not clear whether the resulting sensor configurations are even likely to be feasible for real environments. Moreover, the notation does not allow for modelling any system-level characteristics.

H. Chen and others [7] use Network Simulator NS2 to simulate their experimental network. The whole network consists of 180 nodes, where node 0 represents the outside world, nodes 1 to 19 are the routers interconnecting various parts of the network, nodes 20 to 39 are servers offering valuable services to users and therefore critical assets that need to be protected, and nodes 40 to 180 are ordinary clients some of which may be compromised by intruders to attack critical assets. The network is organised as such that the servers are distributed over six subnets and the clients are distributed over seven separate subnets [6].

3. SENSOR DEPLOYMENT CONSIDERATION

IDS sensors form the eyes and ears of any network (such as Cisco IDS) intrusion detection system. Placing sensors correctly throughout the network is crucial to successfully implementing the intrusion detection system. Before deploying sensors however, administrator must thoroughly understand the network topology, as well as the critical systems on the network that attackers will attempt to compromise [8]. Even after the location is identified on the network where it was planned to deploy sensors, it is still needed to decide on how to configure these sensors to maximize their effectiveness toward protecting the network [9]. The sensor deployment considerations are as follows.

1. Analyse Network Topology

Before beginning to decide where to deploy IDS sensors on the network, analysis of the network topology must be done. Some of the key factors to consider when conducting this analysis are the following:

- Internet entry/access points
- Extranet entry points
- Remote access
- Intranet separation

Almost all networks provide some type of connectivity to the Internet. This connectivity, however, is also a prime target for millions of potential attackers. Therefore, the first place that should be protected on the IDS is the organization's Internet connection. When analyzing connections with the Internet, it is easy to stop at the main Internet access point.

To correctly protect the network, however, it is of need to make sure to identify all possible Internet connections [8].Once the Internet entry points are identified, one need to determine the connections with other organizations. These connections are sometimes referred to as extranet connections [9]. These connections are usually associated with business partners or other organizations that the organization needs to communicate with on a regular basis. These connections open up the network to attack via the organizations that conduct business with. It also opens up the possibility that an attacker can attack these organizations via one's network, which opens up many interesting legal issues [9].

More and more employees are starting to telecommute [10]. Furthermore, more employees also need to maintain access to their local networks when they are travelling. Both of these situations require administrator to establish some form of remote access capability on the network. Remote access, however, is another prime target for attackers [10]. Mapping out all of the remote access entry points into the networks is vital to successfully securing the network against attack. This includes all modems connected to the network.

The final area that needs to be analyzed on the network topology deals with internal separation points. Most organizations are divided into multiple departments [9]. Each of these departments probably shares some common servers, such as DNS and email. Similarly, these organizations usually utilize some departmental servers that should be accessed only by specific users. To enforce the organization's security policy, administrators must clearly understand where these departmental boundaries lie. Furthermore, it must be clearly understood what traffic is allowed and what traffic is not allowed to cross these internal barriers.

2. Critical Components

After analysing the network topology, it should have a clear understanding of how an attacker can gain access to the network (both internal and external attackers). The next thing to do is to define the critical components on the network. These systems represent highly prized targets for an attacker [9]. These are:

Servers

Although every network is unique, there are some common categories of critical machines to start with in analyzing the specific network. The first category is servers. Every network has a multitude of different servers. Some common examples include Mail servers, DNS servers, DHCP servers, NFS servers, and Web servers [9].

Infrastructure Components

The second category of critical systems is the infrastructure components. These components include the routers and switches. These devices enable the hosts on the network to communicate with each other. By gaining control of any of the infrastructure components, an attacker can severely disrupt the operation of the operating network [9].

Security Components

A final category of devices includes the security components that protect the network. These components include devices such as firewalls and IDS components. Because these devices are used to protect the network from attack, they need to be thoroughly hardened against attacks. If an attacker can compromise any of the devices protecting the network, it is difficult to prevent him from compromising others systems on the network as well [9].

3. Deployment

Considering where to place the IDS sensors on the network to watch for potential hostile activity is next on the agenda. To provide thorough IDS coverage of the network, administrators need to watch for intrusive activity at all of the common functional boundaries on the network [9]. Figure 1 illustrates a typical network configuration.

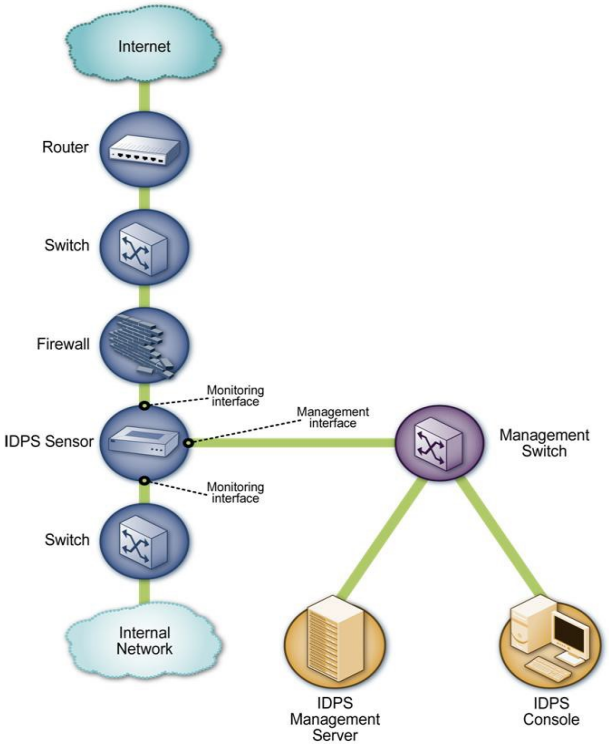

Figure 1 Typical Inline Network-Based IDPS Sensor Architecture [1]

4. Installation Configurations

Having determined the locations on the network at which to install IDS sensors, it is then decided what sensor configuration to use at each of these locations [9]. The common installation configurations are as follows: Standalone sensor, Device management, Firewall sandwich, Remote sensor and Standalone Sensor Configuration [9].

In a standalone sensor configuration (see Figure 2), the sensor watches for intrusive traffic, but has limited capability to react to the attacks detected. It can perform IP Logging to capture a history of the intrusive traffic; and if the attack is TCP-based, then the sensor can generate TCP resets in an attempt to halt the intrusive activity.

In the standalone configuration, the sensor usually communicates alarms and other information to the Director via a separate command and control network connection, as illustrated in Figure 2.

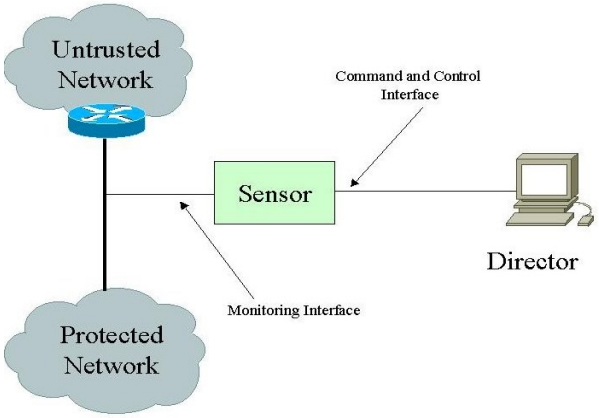

Figure 2 Standalone sensor configuration [9].

Device Management Sensor Configuration

The standalone configuration is fairly limited in the response that it can take with respect to attacks against the network. A more robust configuration includes the device management sensor configuration. In this configuration (also known as IP blocking), the IDS sensor gains the capability to dynamically update an Access Control List (ACL) on the router to halt current and future attacks from the source IP address that is attacking the network. In this configuration, the IDS sensor detects attacks against the network, and generates alarms based on the attack signatures that are observed. If any of these signatures is configured for IP Blocking, then the sensor telnets into the router to automatically block the offending host by updating the ACL [9].

Firewall Sandwich Sensor Configuration

Network administrators typically use firewalls to protect the perimeters of their networks. These firewalls are used to limit the flow of traffic into and out of the protected network [9]. Therefore, placing a sensor to monitor the traffic attempting to gain access to the protected network makes perfect sense. It also eliminates the need to use two interfaces on the router when device management is used. This is the preferred IDS sensor installation configuration [9].

When deploying a sensor in conjunction with a firewall, the administrator can create what is commonly called the firewall sandwich sensor configuration. In this configuration, the IDS sensor is watching traffic on the outside of the firewall. The command and control interface is connected to either the internal firewall network or a DMZ network on the firewall, with the firewall being sandwiched in the middle. When attacks are detected, the sensor can telnet out through the firewall to perform IP blocking on the router located outside of the firewall [9].

Remote Sensor Configuration

The final sensor configuration that we will examine is known as the remote sensor configuration. In this configuration, the administrator needs to operate a sensor on a remote network. This means that he must protect the traffic from the sensor as it travels to the Director because the traffic will be travelling over an untrusted network. A common way to accomplish this goal is to establish a Virtual Private Network (VPN) across the untrusted network. The VPN protects all of the communication between the sensor and the Director [9].

4. SENSORS PLACEMENT IN NIDS

Each IDPS technologies (i.e. network-based, wireless, network behaviour analysis and host-based) has different components and architecture. Based of the difference in the architecture, this study proposed a strategic way of deploying the components especially the sensors to optimally detect and prevent intrusions on Network-Based IDS.

4.1 NETWORK-BASED IDPS

A typical network-based IDPS is composed of sensors, one or more management servers, multiple consoles, and optionally one or more database servers (if the network-based IDPS supports their use) [1]. All of these components are similar to other types of IDPS technologies, except for the sensors. A network-based IDPS sensor monitors and analyzes network activity on one or more network segments. The network interface cards that will be performing monitoring are placed into promiscuous mode, which means that they will accept all incoming packets that they see, regardless of their intended destinations [1]. Most IDPS deployments use multiple sensors, with large deployments having hundreds of sensors. Sensors are available in two formats:

Appliance- An appliance-based sensor is comprised of specialized hardware and sensor software. The hardware is typically optimized for sensor use, including specialized NICs and NIC drivers for efficient capture of packets, and specialized processors or other hardware components that assist in analysis. Parts or all of the IDPS software might reside in firmware for increased efficiency.

Appliances often use a customized, hardened operating system (OS) that administrators are not intended to access directly.

Software Only- Some vendors sell sensor software without an appliance. Administrators can install the software onto hosts that meet certain specifications. The sensor software might include a customized OS, or it might be installed onto a standard OS just as any other application would.

Network Architectures and Sensor Locations

Organizations should consider using management networks for their network-based IDPS deployments whenever feasible. If an IDPS is deployed without a separate management network, organizations should consider whether or not a VLAN is needed to protect the IDPS communications.

In addition to choosing the appropriate network for the components, administrators also need to decide where the IDPS sensors should be located. Sensors can be deployed in one of two modes [10]:

i. Inline. An *inline sensor* is deployed so that the network traffic it is monitoring must pass through it, much like the traffic flow associated with a firewall. One way to achieve an inline sensor is to combine NIDS sensor logic with another network device, such as a firewall or a LAN switch [11] while others are simply IDPSs. The primary motivation for deploying IDPS sensors inline is to enable them to stop attacks by blocking network traffic [10]. Inline sensors are typically placed where network firewalls and other network security devices would be placed—at the divisions between networks, such as connections with external networks and borders between different internal networks that should be segregated. This approach has the advantage that no additional separate hardware devices are needed; all that is required is NIDS sensor software. An alternative is a stand-alone inline NIDS sensor [11]. Inline sensors that are not hybrid firewall/IDPS devices are often deployed on the more secure side of a network division so that they have less traffic to process. Figure 3-1 shows such a deployment. Sensors can also be placed on the less secure side of a network division to provide protection for and reduce the load on the dividing device, such as a firewall.

ii. Passive. A *passive sensor* is deployed so that it monitors a copy of the actual network traffic; no traffic actually passes through the sensor. Passive sensors are typically deployed so that they can monitor key network locations, such as the divisions between networks, and key network segments, such as activity on a demilitarized zone (DMZ) subnet [11]. Passive sensors can monitor traffic through various methods, including the following:

- Spanning Port. Many switches have a *spanning port*, which is a port that can see all network traffic going through the switch. Connecting a sensor to a spanning port can allow it to monitor traffic going to and from many hosts. Although this monitoring method is relatively easy and inexpensive, it can also be problematic [1]. If a switch is configured or reconfigured incorrectly, the spanning port might not be able to see all the traffic. Another problem with spanning ports is that their use can be resource-intensive; when a switch is under heavy loads, its spanning port might not be able to see all traffic, or spanning might be temporarily disabled. Also, many switches have only one spanning port, and there is often a need to have multiple technologies, such as network monitoring tools, network forensic analysis tools, and other IDPS sensors, monitor the same traffic [1].

– **Network Tap.** A *network tap* is a direct connection between a sensor and the physical network media itself, such as a fibre optic cable. The tap provides the sensor with a copy of all network traffic being carried by the media. Installing a tap generally involves some network downtime, and problems with a tap could cause additional downtime. Also, unlike spanning ports, which are usually already present throughout an organization, network taps need to be purchased as add-ons to the network.

– **IDS Load Balancer.** An *IDS load balancer* is a device that aggregates and directs network traffic to monitoring systems, including IDPS sensors. A load balancer can receive copies of network traffic from one or more spanning ports or network taps and aggregate traffic from different networks (e.g., reassemble a session that was split between two networks). The load balancer then distributes copies of the traffic to one or more listening devices, including IDPS sensors, based on a set of rules configured by an administrator. The rules tell the load balancer which types of traffic to provide to each listening device [10]. Common configurations include the following:

- **Send all traffic to multiple IDPS sensors.** This could be done for high availability or to have multiple types of IDPS sensors perform concurrent analysis of the same activity.
- **Dynamically split the traffic among multiple IDPS sensors based on volume.** This is typically done to perform load balancing so that no sensor is overwhelmed with the amount of traffic and corresponding analysis.
- **Split the traffic among multiple IDPS sensors based on IP addresses, protocols, or other characteristics.** This could be done for load balancing purposes, such as having one IDPS sensor dedicated to Web activity and another IDPS sensor monitoring all other activity. Splitting traffic could also be done to perform more detailed analysis of certain types of traffic (e.g., activity involving the most important hosts).

Splitting traffic among multiple IDPS sensors can cause a reduction in detection accuracy if related events or portions of a single event are seen by different sensors. For example, suppose that two sensors each see different steps of an attack; if each step is considered benign on its own but the two steps in sequence are malicious, then the attack might not be recognized [10].

Figure 3 shows examples of passive sensors connected to the monitored network using IDS load balancers, network taps, and spanning ports.

Most techniques for having a sensor prevent intrusions require that the sensor be deployed in inline mode, not passive. Because passive techniques monitor a copy of the traffic, they typically provide no reliable way for a sensor to stop the traffic from reaching its destination. In some cases, a passive sensor can place packets onto a network to attempt to disrupt a connection, but such methods are generally less effective than inline methods. Generally, organizations should deploy sensors inline if prevention methods will be used and passive if they will not [1].

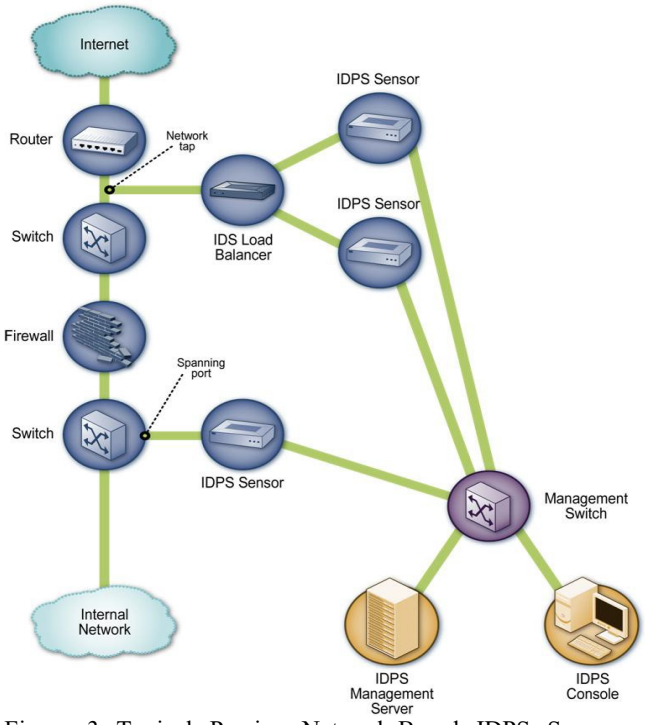

Figure 3 Typical Passive Network-Based IDPS Sensor Architecture [1]

5. SYSTEMS AND NETWORKS TO WATCH

Though it is not realistic to expect to watch all traffic between all systems on the network effectively with NIDS, prioritization of organisation systems and networks is necessary [12].

The systems that provide services to the Internet are a good first choice to watch. These systems are more at risk than systems on your internal network. They also may be providing services to the customers or business partners that are very important to the goals of the organization. It is important to segregate any systems that provide services to the public Internet in a separate network that has limited access to your internal network [12]. This arrangement makes watching the traffic much easier. Other places are as follows:

- There are also a group of servers to watch that provide services to people sitting at the desks, such as print servers, file servers, authentication and directory servers, mail servers, intranet servers, and databases.
- Watching internal LAN traffic is also necessary for it increases the incidence of false positives greatly.
- High-value systems (such as, database storing the ERP solution or the accounting systems) needs targeting for NIDS sensor vigilance.
- The workstations, laptops, and other member of the internal network should not be ignored. It is suggested that traffic between these systems and the Internet be watched by an NIDS.
- If there is a link between WAN connections to business partners or branch offices then a sensor watching traffic is advised.

- A disciplined system administrator is important in the organisation to follows best practices when building the systems, pervasively using antivirus software, and auditing system logs.

The exact placement of sensors is made easier by looking for natural bottlenecks—connections between networks make very nice connection points. The point (or points) that the network connects to the Internet is an easy choice. As previously mentioned, WAN links are important bottlenecks to watch. Considering putting the internal servers on a separate network is essential so that traffic between the networks containing desktop users and servers can be aggregated and watched [12].

6. SECURING THE SENSOR ITSELF

It should be obvious that protecting the integrity of the systems responsible for monitoring and maintaining the security of your network is very important [12]. It is important to protect the integrity not just of the NIDS systems but of the syslog servers, authentication servers, monitoring, and management tools. One important strategy is a management network. This network is behind its own firewall and access to the systems contained within the management network is closely controlled [12]. The systems inside do not even participate in the same authentication domains as the systems on the inside of the network. The only openings in the firewall are those that are needed to get monitoring traffic to the systems that watch the environment [12].

Closely managing the IDS (e.g. snort) system is important. The operating systems should be configured according to industry-accepted best practices and should be kept up-to-date with patches and updates [12].

7. DEPLOYMENT PROBLEMS

When talking about sensors placement on the network it is noteworthy to mention some of the problems encountered.

Based on the problems typically found during sensors deployments a “problem” is defined as a behavior of a set of nodes that is not compliant with a (informal) specification [13].

According to [13] problems are classified according to the number of nodes involved into four classes: *node problems* that involve only a single node, *link problems* that involve two neighbouring nodes and the wireless link between them, *path problems* that involve three or more nodes and a multi-hop path formed by them, and *global problems* that are properties of the network as a whole.

Node Problems

A common node problem is node death due to energy depletion either caused by “normal” battery discharge [13], short circuits or excessive leakage due to inadequate or broken packaging [13].

Link Problems

Field experiments demonstrated a very high variability of link quality both across time and space resulting in temporary link failures and variable amounts of message loss. Interference in office buildings can considerably affect the packet loss; the source often cannot be determined [13].

Path Problems

Many sensor network applications rely on the ability to relay information across multiple nodes along a multi-hop path. In particular, most sensor applications include one or more sink nodes that disseminate queries or other tasking information to sensor nodes and sensor nodes deliver results back to the sink. Here, it is important that a path exists from a sink to each sensor node, and from each sensor node to a sink [13].

Global Problems

In addition to the above problems which can be attributed to a certain subset of nodes, there are also some problems which are global properties of a network. Several of these are failures to meet certain application-defined quality-of-service properties. These include low data yield, high reporting latency, and short network lifetime [13].

8. EXTENDED SENSOR PLACEMENT IN NIDS

Examining Figure 4, it would be seen that the major areas of consideration to place IDS sensors are: Perimeter protection, Extranets, Remote access and Intranets.

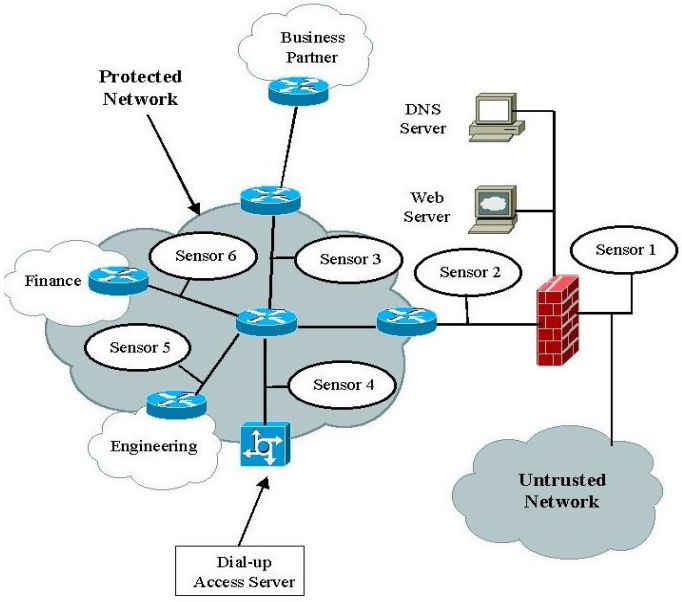

Figure 4 Extended Sensors Placement in NIDS [9]

Sensors 1 and 2 in Figure 1 are watching the perimeter of the network. Usually, this perimeter is protected by a firewall. Therefore, Sensor 1 is located outside the firewall so that it can monitor all the attacks that are launched against the network from the untrusted network. Sensor 2 (the extended sensor that doubled the security) is also watching for attacks against the network from the untrusted network. However, it will only observe attacks that have successfully penetrated the firewall.

Sensor 3 in Figure 4 is positioned to monitor the traffic between the protected network and a business partner's network. Any attacks originating from a business partner (or launched from the network) will be observed by this sensor. Sensor 4 provides this same protection, but for traffic originating from the remote access users [9].

Sensors 5 and 6 in Figure 4 illustrate the way IDS sensors can be used to monitor the flow of traffic between different internal groups on the network. Sensor 5 is protecting the Engineering network, whereas Sensor 6 is protecting the Finance network.

9. CONCLUSION

IDS use sensors to monitor the network for signs of intrusive activity. Understanding where to install the IDS sensors requires a thorough understanding of the organisation network topology, as well as the critical systems. An installation configuration for each IDS sensor must be chosen to provide the level of protection that the network demands. After following all of these steps, however, the IDS will be able to effectively monitor the entire network for intrusive activity. The nature of sensor placement problem is such that there are too many criteria to consider when making a cost effective decision. This study revealed the importance of strategic placement of sensors. The work presented in this paper is to assist network administrators to choose IDS sensor placement that effectively satisfies multiple criteria. The placement strategies generated, although simple, at typical places that network administrators would likely deploy IDS sensors but it suggested additional method which combine firewalls with IDPS sensor for strong and cost effective security to the enterprise resources.

REFERENCES

[1] NIST SP 800-92, *Guide to Computer Security Log Management*, available at http://csrc.nist.gov/publications/nistpubs/

[2] Rolando, M., Rossi, M., Sanarico, N., Mandrioli, D.: A formal approach to sensor placement and configuration in a network intrusion detection system. In: SESS 2006: Proceedings of the 2006 international workshop on Software engineering for secure systems, pp. 65–71. ACM, New York (2006).

[3] *The BSD Syslog Protocol*, http://www.ietf.org/rfc/rfc3164.txt.

[4] NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, http://csrc.nist.gov/publications/nistpubs/

[5] Alan Mainwaring et al, Wireless Sensor Networks for Habitat Monitoring

[6] Noel, S., Jajodia, S.: Attack graphs for sensor placement, alert prioritization, and attack response. In: Cyberspace Research Workshop. (2007)

[7] H. Chen et al, 2009. A Multi-objective Optimisation Approach to IDS Placement. Springer Berlin Heidelberg. http://link.springer.com/chapter/10.1007%2F978-3-642-04091-7_13#page-1

[8] The Placement of IDS Sensors. Briefing Paper by Kevin Graham. http://www.idsec.co.uk/about/briefings/ids-sensor-placement.html

[9] http://www.ciscopress.com/articles/article.asp?p=25327 &seqNum=4

[10] Yi Zou and Krishnendu Chakrabarty (2003). Sensor Deployment and Target Localization Based on Virtual Forces. IEEE INFOCOM 2003

[11] William Stallings & Lawrie Brown. Computer Security: Principles and Practice. Published Aug 2, 2007 by Prentice Hall. ISBN-13: 978-0-13-600424-0. 1st Edition.

[12] http://82.157.70.109/mirrorbooks/snortids/0596006616/snortids-CHP-5-SECT-5.html

[13] Jan Beutel et al. Deployment Techniques for Sensor Networks. citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.156.3388

Author's Brief

Babatunde O. Lawal is a lecturer in Computer Science at the Olabisi Onabanjo University Consult, Ibadan, Nigeria. He received his Master of Computer Systems (MCS) degree from University of Ibadan, Nigeria. He has worked for Trans International Bank as IT Support Officer and Database Administrator. His research interests are Database Management, Data Mining, Information Systems Management and Network Security. You can contact him at lawal5@yahoo.com.

Mr. Ayobami Ibitola lectures at the Department of Computer & Information Sciences, Lead City University, Ibadan, Nigeria. He holds the Bachelor's and Master's degree in Computer Science from the Department of Computer Science, University of Ibadan, Ibadan, Nigeria in 2006 and 2009 respectively. His research focuses on intelligent and knowledge-based systems, ICT diffusion and system interoperability, He can be reached at ibitolaayobami@yahoo.com or on phone through +2348035135700.

Longe Olumide (PhD) is on Faculty at the Department of Computer Science, University of Ibadan, Nigeria. His research has focused on using social theories, machine learning and computer security models to design cyber security systems and explain cyber victimization. He can be reached at longeolumide@fulbrightmail.org