AN EFFICIENT INTRUSION DETECTION SYSTEM FOR NETWORKS WITH CENTRALIZED ROUTING

Paulo F. Andrade, Fernando Mira da Silva and Carlos Ribeiro
Instituto Superior Técnico, Universidade Técnica de Lisboa, Lisboa, Portugal

Keywords: Intrusion Detection Systems, Switch-based Networks, Security Analysis.

Abstract: As Internet becomes more and more ubiquitous, security is an increasingly important topic. Furthermore, private networks are expanding and security threats from within the network have to be cautioned. For these large networks, which are generally high-speed and with several segments, Intrusion Detection System (IDS) placement usually comes down to a compromise between money invested and monitored services.

One common solution in these cases, is to use more than one IDS scattered across the network, thus, raising the amount invested and administrative power to operate. Another solution is to collect data through sensors and send it to one IDS via an Ethernet hub or switch. This option normally tends to overload the hub/switch port where the IDS is connected.

This paper presents a new solution, for networks with a star topology, where an IDS is coupled to the network's core router. This solution allows the IDS to monitor every different network segment attached to the router in a round-robin fashion.

1 INTRODUCTION

Over the past two decades, with the rapid growth of the Internet — which now counts with more than 100 million sites (Netcraft, 2006) — companies have been forced to change the way they do business. To keep up with new Internet-centric companies or simply to still be competitive, many companies have had to alter their business process to accommodate this new means of communication.

However, along with this growth, the number of attacks to Internet sites has also increased dramatically. For instance, between 2000–2006, the number of incidents reported to Computer Emergency Response Team Coordination Center (CERT/CC) grew around 740%.

There are a few factors that contribute to this astonishing rate. First, there is the continuously publication of exploits and vulnerabilities on the Internet as they are discovered. Secondly, there is a profusion of intrusion tools and automated scripts available that duplicate known methods of attacks. These two factors combined allow for practically anyone with little technical knowledge to be able to perform an attack. Consequently, the number of sophisticated attacks has increased.

This paper starts by defining ”intrusion detection” in section 2. Then, section 3 describes the common solutions for Intrusion Detection System (IDS) placement together with their benefits and drawbacks. The proposed solution is described in section 4. And, finally, section 5 concludes.

2 INTRUSION DETECTION SYSTEMS

Although the word ”intrusion” might connote a successful attack, Intrusion Detection Systems are used to detect anomalies, regardless of them being intentional or not. There are several definitions for ”intrusion detection”, one widely accepted is presented in (Rich, 2005): ”Intrusion detection is the methodology by which undesirable or aberrant activity is detected on a host or a network.”

Under this broad definition, all undesirable or abnormal activity might be considered an intrusion, being it planned or not. A Denial-of-Service (DoS) (Ptacek and Newsham, 1998) attack, an user infected

F. Andrade P., Mira da Silva F. and Ribeiro C. (2007).
AN EFFICIENT INTRUSION DETECTION SYSTEM FOR NETWORKS WITH CENTRALIZED ROUTING.
In *Proceedings of the Second International Conference on Security and Cryptography*, pages 102-106
DOI: 10.5220/0002127001020106

by a virus that is using the local mail server to send spam, or a buggy Transmission Control Protocol (TCP) stack in an Operating System (OS) that is incorrectly fragmenting packets are a few examples of possible intrusions.

IDSs are usually divided into two major categories, Host-based Intrusion Detection Systems (HIDSs) and Network-based Intrusion Detection Systems (NIDSs) (Singh, 2005). This paper focuses on NIDS.

3 CONVENTIONAL IDS PLACEMENT

IDS placement is one of the most important aspects in the design of a secure network infrastructure. The balance between monitoring coverage and resources allocated is not an easy subject. This is specially true when dealing with network-based IDS. For HIDSs, the decision is relatively easier. Host-based IDS should, usually, be placed on the hosts that provide services crucial to the organisation.

The next subsections discuss the rationale behind the design of the proposed solution. Starting from small and rather simplistic networks and building up to large and more complex networks.

3.1 Basic Network Setups

Usually small to medium-sized networks use a setup consisting of a central switch connecting the gateway and other computers/segments. Instead of the switch hardware, there might be an ethernet hub. Using a shared-medium also implies that all devices connected to the hub will listen to all the networks traffic that flows through it. In this scenario an IDS may simply be connected to the hub to be able to monitor the entire network (assuming that there are no switches on either segments). This scenario is, however, rather simplistic.

When using a network switch, packets arriving in one port are sent to the port where the packet's target might be found. In this scenario, simply connecting a NIDS to a port on the switch won't suffice, since all traffic routed to the other ports won't be monitored, namely the traffic going to and from the gateway.

There are mainly three ways that allow one to use a NIDS to monitor traffic leaving and entering the network. Note that, in this section, it is assumed that the network is trusted (which is generally the case for small to medium sized networks), and therefore monitoring traffic between network devices is not necessary.

Hubs Due to its properties, using a hub between the switch and the gateway allows all incoming and outgoing traffic to be copied off to the IDS. This is a simple and inexpensive way to go about solving this problem. However hubs can easily degrade network performance, therefore this solution is presented merely as an example.

Taps The tap solution is very similar to the hub. A network tap is a hardware device which provides a way to access the data flowing across a link. Taps have at least three ports; the A and B port are used to establish the connection between the two network segments; the remaining ports, also called monitor ports, are used to connect the IDS. One important aspect to note, is that if the network link is an 100 mbps full-duplex link, then the aggregate traffic comprising of the traffic in both directions would be 200 mbps. This is a problem if the tap only has one monitor port. In these cases, taps usually have two ports that monitor each direction of the traffic; the IDS can use channel bonding to monitor all traffic. Furthermore, taps don't interfere with the communication link between the two segments. Also, good taps are fault tolerant, the connection between ports A and B is hardwired in, which means that in case of a power failure the communication link between the two connected segments will not be broken.

Port Mirroring This solution depends on the switch capabilities, namely if port mirroring is an available feature. It consists on replicating data from one or more ports onto a single port, referred as the monitoring port. This feature is also known as: Monitoring Port, Spanning Port, Switch Port Analyzer (SPAN) port and Link Mode port. In this setup the switch can be configured to copy the traffic passing through the port where the gateway is connected, to the monitoring port. Both directions (TX and RX) of the traffic are copied, thus achieving the same monitoring capabilities of the previous solutions.

3.2 Medium and Large Network

In large networks, IDS placement is a much more complex task, specially if the network is a public or easily accessible at the physical level (such as Universities, e.g.). There are several hundred of installed workstations, various points where laptops can be connected to the network and, more recently, wireless access points for users to connect their laptops or Personal Digital Assistants (PDAs).

With this scenario, simply monitoring the Internet connection is not enough, attacks perpetrated by attackers inside the network would not be detected. This is an important issue, specially when users can bring their own machines which the network and system managers have no control over.

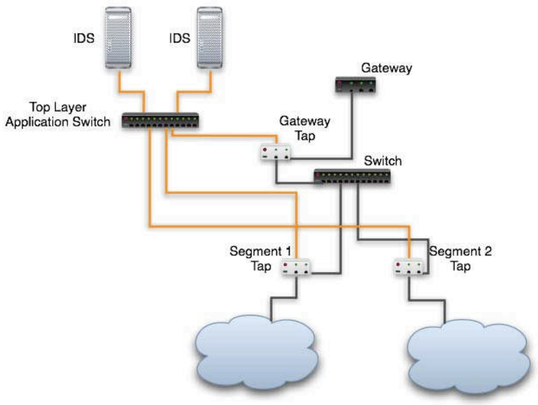

Figure 1: Consolidating the taps output with a Top Layer Application Switch which is, in turn, balancing the load to two IDSs
Note: Actually there should be two lines connecting the taps and the Top Layer Application Switch, one for each traffic direction (RX and TX).

The example shown in Fig. 1 is a simple example of monitoring more than one network segment. Two network segments are connected by a tap to a Top Layer Application Switch (TLAS) which in turn is connected to one or more IDSs.

Normal packet switching involves looking at a packet headers, whether it is the layer-2 headers, in the case of switching based on the Media Access Control (MAC) address, or layer-3, in case of switching based on the Internet Protocol (IP) address. In either case, the forwarding decision can be made by looking at a single packet. A TLAS (Kessler, 2001) differs from conventional switches in the sense that it makes its decisions based on flows rather than single packets.

Because IDS machines must monitor both directions of a flow, this switch awareness is crucial. The notion of flows allows the TLAS to send both TX and RX streams to one IDS — this is called flow mirroring. The TLAS can effectively balance the traffic load collected from the taps to various IDS machines, radically diminishing the possibilities of overloading the port where the IDS is connected.

Of course, one could exclude the TLAS and use several NIDS, one for each tap. But this would be much more costly.

4 NETWORKS WITH CENTRALIZED ROUTING

Networks which have a star topology are one of the most commons. In this topology, a central node acts as a router for all the attached network segments. This node might be a switch, a router or even a computer. Note that the attached segments can be any type of sub-network, including wireless networks.

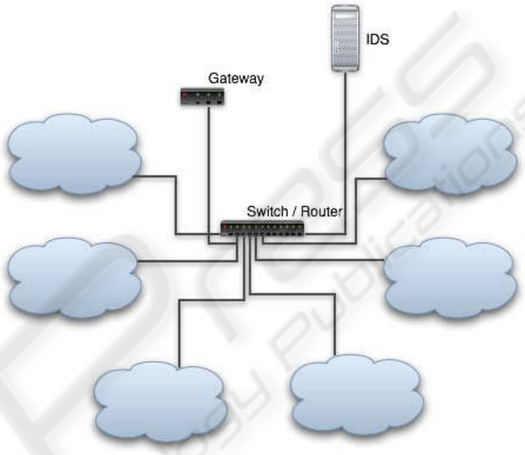

Figure 2: Example of a network with a star topology, where the IDS is connected directly to the central node.

For these networks, if a decision was required regarding which network segments should be monitored by a network-based IDS, a common conclusion would be to monitor all segments that are connected to the central node, or a subset of these (only those that are considered relevant or vulnerable). One could place a tap on those segments and use the approach described in the previous section. However this paper suggest a different approach, one that dispenses the use of taps and a Top Layer Application Switch altogether.

Attacks aren't instantaneous. Port scanning, network topology discovery, OS *fingerprinting*, DoS attempts, running exploits, etc. Attacks consist of several steps, many of which can take a considerable amount of time.

Therefore, sampling the network traffic from each of the segments attached to the central node in a round-robin fashion may be effective. Meaning that there is time for the IDS to rotate trough all the ports while the attack is in action; it is a matter of calibrating the time between hops with respect to the number of segments to monitor. Provided that doing this might prove to be rather difficult. There is no formula for calculating the average time an attack takes to occur, so calibrating this value will be based on testing and the knowledge about current common attack times.

Common routers and switches facilitate their management by either a Secure Shell (SSH) connection (older devices use telnet) and/or through Simple Network Management Protocol (SNMP) queries. The idea is to let the IDS monitor all, or any subset, of the segments connected to the router, one by one, in a round robin fashion. If any suspicious activity is detected on the port being monitored, the IDS will stick to that port and emit appropriate warnings or take the appropriate actions. Once the suspicious activity has terminated for a configurable amount of time or if an administrator so wishes, the IDS will return to its normal cycle of operation.

Also, if the router is able to mirror more than one port at a time, the system could be configured to keep monitoring one or more ports (the port connected to the Internet, e.g.) and cycle through the others — provided that the aggregate traffic does not overflow the monitoring port.

The advantages of this solution are:

- No further hardware needed. Provided that the current central router/switch has port mirroring capabilities;
- Since the IDS is usually only monitoring one port at a time, there is a low risk of the monitoring port being overloaded.
- It is flexible. Many routers allow for mirroring of more than one port at a time, the system can be configured to keep monitoring the port where the gateway is connected, or keep monitoring the port where suspicious activity was detected and continue to monitor the other ports in a round-robin fashion.

And the drawbacks are:

- Only segments attached to the central node can be monitored;
- Can not monitor all segments all the time, due to the risk of overloading the monitoring port.

This approach requires developing the software that will control the router and integrate with the IDS; one such as Snort (Sourcefire, 2006) for example. To be able to interact with the router, in case it does not allow for the device connected to the monitoring port to transmit, the IDS has to have two network cards, both connected to the router. One for the traffic being mirrored and the other to allow the IDS to communicate with the router and control which port is being mirrored.

5 CONCLUSION

To achieve a proper intrusion detection infrastructure, a mixture of host-based IDS and network-based IDS is needed. Both have complementary characteristics. For instance, in encrypted network environments, HIDS are more effective since they act after the traffic has been decrypted. Conversely, for real-time detection, NIDS are more effective.

A common setup is to have NIDS monitoring entry points of the network, and all segments that might present further risks — such as those that facilitate wireless connectivity —, and to have HIDS at critical servers.

The proposed solution brings another way to place a NIDS on the network. One that makes a new compromise between the money invested and monitoring ability. On one side of the scale, it is easy to see that implementing such a solution would be cheaper than those which involve using other hardware, such as taps and TLAS, and since there is only one IDS to maintain, management costs are also reduced. However, on the other side of the scale, this solution should only be considered on networks with central routing, and the fact that not all the segments are being monitored at one time might not be an option for everyone.

REFERENCES

Kessler, G. C. (2001). IDS-in-Depth: Top Layer's App-Switch filters a copy of traffic flows to downstream IDSeS. *Information Security Magazine*.

Netcraft (2006). November 2006 Web Server Survey. http://news.netcraft.com/archives/2006/11/01/november_2006_web_server_survey.html – Avail. November, 2006.

Ptacek, T. H. and Newsham, T. N. (1998). Intursion, Evasion and Denial of Service: Eluding Intrusion Detection.

Rich, A. (2005). Introduction to Intrusion Detection With Snort. http://www.sun.com/bigadmin/features/articles/intrusion_detection.html – Avail. December, 2006.

Singh, K. K. (2005). *Intrusion Detection and Analysis*. PhD thesis, University of British Columbia.

Sourcefire (2006). Snort. http://www.snort.org/ – Avail. April, 2007.

ACRONYMS

IDS	Intrusion Detection System
CERT/CC	Computer Emergency Response Team Coordination Center
DoS	Denial-of-Service
TCP	Transmission Control Protocol
OS	Operating System
HIDS	Host-based Intrusion Detection System
NIDS	Network-based Intrusion Detection System
MAC	Media Access Control
SPAN	Switch Port Analyzer
IP	Internet Protocol
PDA	Personal Digital Assistant
TLAS	Top Layer Application Switch
SSH	Secure Shell
SNMP	Simple Network Management Protocol