

IDS location for real time network protection .

C.A. de la Torre

Departamento de Ciencias de la Computación, Escuela Politécnica del Ejército, Sangolquí, Ecuador

INTRODUCTION: An intrusion into an information system tries to compromise the security of the system. Intrusion Detection System (IDSs) attempt to detect these intrusions, so optimal allocation of Intrusion Detection Systems is essential to improve network security. Knowing what is being accessed on the network and how it is being accessed is key to providing a secure and compliant network. The ability to find a few key frames in large stream of data is necessary to determine the source of unauthorized access. However, it is important to ensure the internal security of your network as it to ensure the external security. In this work, present the important problem of where to place Intrusion Detection Systems that could detect unauthorized network traffic, improve security in devices that support SNMP and detect restricted documents transfers.

1 PRINCIPAL CAUSES FOR SECURITY RISK

Streaming media, file downloads and chat applications can not only rob bandwidth from mission critical applications, but also pose a security risk. Identifying whether these application and who is using them is part of a systematic security evaluation .

Lack of User Access List on the devices to limit the IP address that can access the devices using SNMP, can be a serious problem in many corporate networks. For instance, the use of default SNMP community strings in devices that can be accessed from unauthorized nodes seriously can compromise network security.

The installation of devices inside corporate networks, without the knowledge of network staff; can represent an open door to network resources for cybercriminal groups. Besides, some network devices may not be properly secured to ensure only authorized access to the network. Such network devices can be exploited by persons outside of the organization for developing cybercriminal actions.

2 INTRUSION DETECTION SYSTEMS

A typical hacker attack is not a simple, one-step procedure. It is rare that a hacker can get online or dial up on a remote computer and use only one method to gain full access. It is more likely that the attacker will need several techniques used in combination to bypass the many layers of protection standing between them and root administrative access. There are many technologies to prevent a security break-up in the systems like Intrusion Detection System, Honey-pots and Firewalls. In this paper will analyze the benefits of figuring out optimal location for IDS. Intrusion Detection Systems can be categorized into three types: host-based IDS, network-based intrusion detection system as well as router-based IDS.

Host-based Intrusion Detection Systems are usually deployed on individual host-machines to monitor activities on the host machines. Since the host-based Intrusion Detection Systems are

deployed in individual host machines, their implementation is machine-dependent, as well as, takes away much of the computing power from the users of the host machines. If the hosts become victims from intrusions, then Intrusion Detection Systems are brought down along with the host machines. Moreover, separate Intrusion Detection Systems on individual host machines do not provide a direct as well as complete picture of distributed intrusions against a network, making it difficult for the SSA (Security System Administrator) to take corrective actions. The main advantage of the host-based Intrusion Detection Systems is that it can detect intrusions targeting the host machines from both insiders as well as outsiders.

Network-based Intrusion Detection Systems are usually set up in computers of strategic importance in the network to keep an eye on information packets sent amid the hosts. Network-based Intrusion Detection Systems can detect breach of network security policy, but may be unable to manipulate information like not only the header part but also the information part of information packets so as to disclose certain intrusive activities for precise detection. Furthermore, huge number of network traffic makes it difficult in competently manipulating such data.

Router-based Intrusion Detection Systems are setup on routing devices to scrutinize information packets going through routers, thus encouraging thwarting intrusive information packets from inflowing the network inside the router. Router-based Intrusion Detection Systems are similar to network-based Intrusion Detection Systems, as well as thus suffer from similar problems.

2.1 Definitions

In this section present the essential definitions for general IDS location, and then present the optimal IDS location problem. First, is considered a wide area network, where the internal nodes are routers and the external nodes are servers, clients or gateways to different subnets. The protection system is represented as follows: s – subjects (users, process), o – objects (system resources, services). The subject s wants access to object o , there exist a protection state that allow or deny this action named IDS. A subject v_s can request for data from any of the objects, v_o , so the protection state allows or denies this action, if the protection system allows this process the server where is installed the object o, v_o , sends data to the subject, v_s , on the shortest path from the object to the subject. When IDS are present any anomaly traffic can be detected in real time, so the cybercriminal subject actions can be blocked in a IDS, v_k , rather than obtain any response data from any object server.

Consequently, the performance of an optimal IDS location scheme is a function of network topology and request model allowing network contacts. Otherwise, the exact behavior of IDS can be achieved analyzing variables such as User Access List, the capture frames at line rate, the quickly determine of who is accessing files, etc.

In next pages will refer to the bytes sent from object to a subject as the flow to the subject. The principal idea in this paper is to figure out the best possible locations for IDS, to achieve this used to a model of the IDS, and replace it with a simple parameter the detection hit rate. The detection hit rate, p , is the fraction of blocked connection by optimal locate IDS. A higher hit rate implies a lower load on the network, and much work has been done analyzing IDS variables to improve detection hit rates.

The reason IDSes are placed in the network is to improve network security and performance, primarily in terms of reducing security risk, and second reducing the load on the network links. From a user point of view, performance is measured by the response time; it is the time that takes data to arrive. For instance, time depends both on the link delays, and on the response time of the object servers. The goal is to minimize the total network flow; it is the sum of all network

flows taken over all the links. This may improve the network security, because eliminate network flows that pose security risk. It is equivalent to minimizing the average delay for user traffic through our network and thus also optimizes the network performance.

2.2 The formal model

The formal model agree with the above definitions, is represented by an undirected graph $G=(V,E)$, where $V= \{v_i\}_{i=1}^{i=n}$ is the set of nodes. E is the set of edges, $d(e)$, the length of the edge e , reflects the delay caused by the edge, and $d(v_i, v_j)$ is the sum of the link distance along the route between nodes v_i and v_j (object and subject respectively). Assume that shortest path routing is used. The request pattern is modeled by the demand set F , so amount of data flowing from o -th node to s -th node should be denoted as f_{os} and p_{os} is the detection hit ratio in that flow. We denote by K the set of at most k nodes where the IDSes are to be placed.

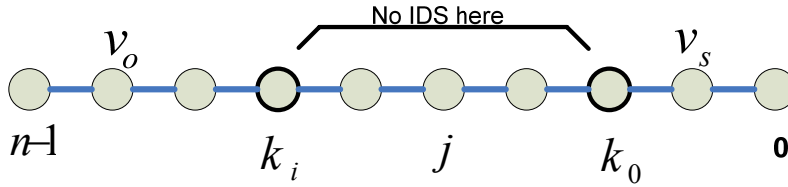


Figure 1: Distribution of K IDS set in an shortest route, between subject v_s and object v_o

Consider a line of n nodes numbered from 0 to $n-1$ of Figure 1. The input is the flow requirements from (up to) n objects located at the nodes to (up to) n subjects also located at the nodes. A node can accommodate both a subject and an object. IDS accommodate in nodes k_i , and k_0 . The network flows between nodes v_s and v_o are composed of mission critical applications flows and security risk flows. The function of IDS is to block the security risk flows and allows the pass of flows from critical applications. So, the request of v_o to v_s requirements is only for mission critical applications. Therefore, the cost c_{oks} of demand f_{os} via IDS in location v_k is:

$$c_{oks} = f_{os} * [d(v_o, v_k) + d(v_k, v_s) - p_{os} * d(v_o, v_k)]$$

An optimal assignment of IDS to block security risk flows is to assign IDS v_k (or not IDS at all), so this allocated IDS block suspicious security risk flows in its influence area. The cost C_{OKS} is minimal among all possible v_k in $K \cup \{v_s\}$. As considered earlier in this paper assumes a full dependency among IDSes. Hence this model does not capture hierarchical structures. So, our overall objective here is to find a set K that minimizes the total cost, it is the sum C of all the cost, $C = \sum_{f_{os} \neq 0} C_{oks}$

The above analyzed task can be formalized in two ways, first as a graph optimization problem and second as a simple optimization problem.

2.3 Graph optimization problem

2.3.1 Problem 1: The general k -IDS location problem

Given:

1. An undirected graph $G=(V,E)$.
2. Set of demands $F: V \times V \rightarrow \text{IN}$
3. Hit detection radio set P
4. Number of IDS k

Solution:

- A subset $K \subset V$ of size k .

Objective: Minimizing the sum of costs:

$$\sum_{o,s} \frac{\min}{v_k \in K \cup \{v_o\}} f_{o,s} * [d(v_o, v_k) + d(v_k, v_s) - p_{o,s} * d(v_o, v_s)]$$

2.3.2 Problem 2: The k -IDS location problem with set of static routes R .

Given:

1. An undirected graph $G=(V,E)$.
2. Set of demands $F: V \times V \rightarrow \text{IN}$
3. Hit detection radio set P
4. Number of IDS k
5. Set of static routes $R = \{\text{static-routes}(v_o, v_s)\}$

Solution:

- A subset $K \subset V$ of size k .

Objective: Minimizing the sum of costs:

$$\sum_{o,s} \frac{\min}{\{v_k \in (K \cup \{v_o\}) \cap R\}} f_{o,s} * [d(v_o, v_k) + d(v_k, v_s) - p_{o,s} * d(v_o, v_s)]$$

2.3.3 Problem 3: The k -IDS location problem with dynamic routes

Given:

1. An undirected graph $G=(V,E)$.
2. Set of demands $F: V \times V \rightarrow \text{IN}$
3. Hit detection radio set P
4. Number of IDS k
5. Number of nodes $n = \|V\|$

Solution:

- A subset $K \subset V$ of size k .

Objective: Minimizing the sum of costs:

$$\sum_{i=0}^{n-1} \sum_{O,S} \frac{\min}{\{v_k \in (K \cup \{v_o\}) \cap \{all - routes(v_o, v_s)\}\}} f_{O,S} * [d(v_o, v_k) + d(v_k, v_s) - p_{O,S} * d(v_o, v_k)]$$

2.4 Generalization of detection hit radio

Analyzing network behavior in constant time periods, similar attacks should be identified in each node. Besides, if equal IDSes are used in k -nodes the analyzed variables for attack detection must be the same in each network point. So, the result of scanning anomalies in any node generated by network flows, in equal time periods, must be similar; assuming that network flows pass for at least one IDS. There exists a constant hit rate p that matches to scanned anomalies. So, the cost equation should be rearranged as follow:

$$c_{oks} = f_{os} * [d(v_k, v_s) + (1 - p) * (d(v_k, v_s) + d(v_o, v_k))]$$

2.4.1 Problem 4: The k -IDS location problem with constant hit detection rate

Given:

1. An undirected graph $G=(V,E)$.
2. Set of demands $F: V \times V \rightarrow \mathbb{IN}$
3. Set of static routes $R = \{static - routes(v_o, v_s)\}$
4. Network detection hit rate p
5. Number of IDS k

Solution:

6. A subset $K \subset V$ of size k .

Objective: Minimizing the sum of costs:

$$\sum_{O,S} \frac{\min}{\{v_k \in (K \cup \{v_o\}) \cap R\}} f_{os} * [d(v_k, v_s) + (1 - p) * (d(v_k, v_s) + d(v_o, v_k))]$$

2.5 Conclusions

Network Intrusion Detection Systems do a good job controlling which traffic is allowed to flow in Internet, However, it is inevitable that some of the traffic that they allow to flow are malicious in nature or are garbage, so each network into Internet needs a second layer of defense, generally a firewall and content filter http, ftp, etc. In addition, the efficiency of this kind of NIDS depends of distance counted in hops to flow source, so undesired flows could be blocked before saturate critical network links.

2.6 Bibliography

1. Allen, J., Christie, A., Fithen, W., McHugh, J., Pickel, J., and Stoner, E., State of the Practice of Intrusion Detection Technologies. CMU/SEI-99-TR-028, Carnegie Mellon University, Software Engineering Institute, January 2000.
2. Anderson, James P., Computer Security Threat Monitoring and Surveillance. James P. Anderson Co., Fort Washington, Pa., 1980.
3. AIDE Manual , <http://www.cs.tut.fi/~rammer/aide/manual.html>.
4. Bace, Rebecca Gurley. (2000). Intrusion detection. Indianapolis, IN: Macmillan Technical Publishing.
5. Bace, Rebecca. Mell, Peter. Intrusion Detection Systems. NIST Special Publication on Intrusion Detection Systems.