Inferring Internet Denial-of-Service Activity

Geoffrey M. Voelker and Stefan Savage

Presented By Ntallaris Efstratios

1 Introduction

In the early 2000's massive Denial of Service (DoS) attacks took place targeting government organizations, educational institutions, etc, and many big companies such as Yahoo, Ebay and Microsoft. At that time there was not much relevant data to characterize DoS attacks. As a result this paper tries to characterize and quantify DoS attacks, by doing a technique called "backscatter analysis".

2 DoS attack types

In denial of service attacks, the attacker tries to consume victim host resources such as network bandwidth, CPU, and memory in order to block the victim to use those resources for legitimate users. There are two main categories in denial of service attacks. The first category is logic attacks. In this type of attacks, the attacker tries to find a software vulnerability and exploit it in order to crash the victim host or degrade its performance. To prevent these type of attacks the victim host must regularly upgrade the faulty software or filter particular packet sequences. The second category is flooding attacks. In this category the attacker sends rapidly fake requests to the victim host in order to overload his resources. Prevention of this attacks is hard, as it is difficult for the victim host to recognize 'bad' packets (the packet that the attacker sends) from 'good' (legitimate) packets. An example of flooding attack is SYN Flood.

![Figure 1: SYN Flood attack](image-url)
In order for a client to establish a TCP connection with a server, a TCP 3-way handshake is taking place. Client sends TCP-SYN, Server allocates memory and replies with TCP-SYN ACK and then again Client replies with ACK to establish a connection. An attacker can take advantage of this by sending TCP SYN to the victim host, and then never sending an ACK. This way the victim host will allocate memory for the connection. If the attacker does this multiple times, he can use all the resources of the victim host. An example can be seen in figure 1. Other flooding attacks are TCP ACK, NUL, RST, DATA floods, IP Fragment floods, ICMP Echo Request Floods, and DNS Request floods.

3 Distributed attacks and IP Spoofing

Usually attackers are doing attacks in a distributed way. They compromise hosts (which are called zombies) install a daemon, and launching attacks to a single site from them. An example can be seen on the next figure:

![Figure 2: Distributed DoS Attack](image)

Another thing that attackers can do is to spoof the source IP Address. Instead of putting their IP address as source address they put other IP Address. An example of IP spoofing can be seen in the next figure.

![Figure 3: IP Spoofing example](image)

For this paper we assume that the source IP address is random.
4 Backscatter analysis

The basic assumption in order for this analysis to work is that the IP Addresses are chosen randomly, and they may not refer to a real IP Address. The monitor has also an address range (of fake IP’s) and checks if the observed addresses are consistent with a uniform distribution of this address range of fake IP’s with a technique called the Anderson-Darling (A2). The monitor actually captures all the backscatter packets.

**Backscatter packets** are the packets that are aimed to do a DoS attack. An example of the backscatter packets can be seen on the next figure:

![Figure 4: Backscatter packets example](image)

As seen on Figure 4 the attacker prepares a syn-flood and sets as IP Source D B and C. When victim receives this packets he sends TCP SYN-ACK to hosts with IP Source D B and C, but he never receives TCP ACK. Some packets were not monitored for the following reasons:

- Some ISP’s do ingress filtering to drop packets with IP Addresses that are outside their range.
- Attackers may use a technique called reflector attacks. The IP Address will not be chosen randomly and the this packets wont get monitored.
- The distribution set of source IP Addresses of an attack was not randomly distributed.
4.1 Detecting a Denial Of Service Attack

In order to detect an attack on the monitor side, the following equation is used:

\[ E(X) = \frac{nm}{2^{32}} \]

Where \( n \) is the number of distinct IP addresses and \( m \) is the number of packets. The monitor can also detect the attack rate of the packets that are being directed to the victim with this equation:

\[ R > R' \frac{2^{32}}{n} \]

where \( R' \) is the median inter-arrival rate of backscatter from the victim and \( R \) is the attack rate described as packets-per-second.

4.2 Attack classifications

The monitor classifies the attacks in two categories. The first category is called Flow Based Classification. Whenever the monitor receives the first packet for each target he opens a time-window (in the paper 5 minute time-window is used) and measures the packets received in that time-window. Information from each packet of a flow is extracted. Some parameters that the log monitor extracts in order to quantify an attack is:

- TCP flag settings
- ICMP payload
- Port settings
- DNS information
- Routing information

Only flows that are at least 60 seconds and have at least 100 packets are accepted.

The second category for classifying attacks is called Event Based Classification. Event Based classification is used to keep information for a periodic time events that the flow based classification cannot quantify. In this category the traces are divided into one-minute time windows. For each one-time windows an attack event is recorded, but in order to record an attack event the monitor must at least gather ten backscatter packets. The goal of this classification is to measure the momentary impact on a particular victim.

Information that can be extracted from this classification type is for example how many different attacks at the same time the attacker established at the victim or the distribution of the attack rates for the attack events.
5 Experimental Framework

Traffic from /8 network was monitored (1/256 of the total internet). Totally 12,805 attacks were detected in a course of a week to 5,000 distinct IP Addresses in more than 2,000 distinct DNS Domains. Almost 200 million backscatter packets were analyzed. Three traces were collected, each trace had backscatter packets of almost a week.

![Figure 5: Estimated number of attacks/hour](image)

In Figure 5 we see the estimated victims of the three traces. On Y axis we see the distinct victims/hour and on X axis the days that the distinct victims were estimated. We can see that the attacks do not follow any pattern on all three traces. We can also see that on February 20th 150 distinct victims were reported, which are the most victims in all three traces.

![Figure 6: Backscatter packet types in all traces](image)

In Figure 6 we see for each trace the backscatter packet type, the total number of attacks and the total packets sent on each attack. On the parentheses we see the relative percentage for each count. We can see that almost 50% of
the attacks and almost 20% of the packets are TCP with the RST and ACK flags set. Next come the ICMP Host Unreachable packets with almost 20% of the attacks.

<table>
<thead>
<tr>
<th>Kind</th>
<th>Trace-1</th>
<th>Trace-2</th>
<th>Trace-3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attacks</td>
<td>Packets (k)</td>
<td>Attacks</td>
</tr>
<tr>
<td>TCP</td>
<td>3,902 (94)</td>
<td>28,705 (56)</td>
<td>3,472 (90)</td>
</tr>
<tr>
<td>UDP</td>
<td>99 (2.4)</td>
<td>66 (0.13)</td>
<td>194 (5.0)</td>
</tr>
<tr>
<td>ICMP</td>
<td>88 (2.1)</td>
<td>22,020 (43)</td>
<td>102 (2.6)</td>
</tr>
<tr>
<td>Proto 0</td>
<td>65 (1.6)</td>
<td>25 (0.05)</td>
<td>108 (2.8)</td>
</tr>
<tr>
<td>Other</td>
<td>19 (0.46)</td>
<td>12 (0.02)</td>
<td>2 (0.05)</td>
</tr>
</tbody>
</table>

Figure 7: Protocols used in attacks

In Figure 7 we see the protocols used in attacks for all three traces. We can see that 90% of the attacks used TCP protocol. We also observe that for ICMP packets a large amount of packets (almost 50%) were sent for only 2% of the attacks.

<table>
<thead>
<tr>
<th>Kind</th>
<th>Trace-1</th>
<th>Trace-2</th>
<th>Trace-3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attacks</td>
<td>Packets (k)</td>
<td>Attacks</td>
</tr>
<tr>
<td>Multiple Ports</td>
<td>2,740 (66)</td>
<td>24,956 (49)</td>
<td>2,546 (66)</td>
</tr>
<tr>
<td>Uniformly Random</td>
<td>655 (16)</td>
<td>1,584 (3.1)</td>
<td>721 (19)</td>
</tr>
<tr>
<td>Other</td>
<td>267 (6.4)</td>
<td>994 (2.0)</td>
<td>204 (5.3)</td>
</tr>
<tr>
<td>Port Unknown</td>
<td>91 (2.2)</td>
<td>44 (0.09)</td>
<td>114 (2.9)</td>
</tr>
<tr>
<td>HTTP (80)</td>
<td>94 (2.3)</td>
<td>334 (0.66)</td>
<td>79 (2.0)</td>
</tr>
<tr>
<td>0</td>
<td>118 (2.7)</td>
<td>256 (1.0)</td>
<td>39 (1.0)</td>
</tr>
<tr>
<td>IRC (6667)</td>
<td>114 (2.7)</td>
<td>526 (1.6)</td>
<td>39 (1.0)</td>
</tr>
<tr>
<td>Auth (113)</td>
<td>54 (0.81)</td>
<td>49 (0.10)</td>
<td>52 (1.3)</td>
</tr>
<tr>
<td>Telnet (23)</td>
<td>17 (1.6)</td>
<td>252 (0.50)</td>
<td>18 (0.46)</td>
</tr>
<tr>
<td>DNS (53)</td>
<td>30 (0.72)</td>
<td>39 (0.08)</td>
<td>3 (0.08)</td>
</tr>
<tr>
<td>SSH (22)</td>
<td>3 (0.07)</td>
<td>2 (0.00)</td>
<td>12 (0.31)</td>
</tr>
</tbody>
</table>

Figure 8: Attacks based on port number(service)

Figure 8 shows the attacks based on service. We can see that most of the attacks focus on multiple ports rather than a single port. Port 0 represents the ICMP Packets. Many popular services that are being attacked are HTTP (80), IRC(6667), Telnet(23), DNS(53) and SSH(22).
Figure 9 shows the cumulative distribution of attack durations. Y axis and X axis are in logarithmic scale. We can see that 80% of the attacks had duration less than 30 minutes. On the tail distribution we can see that 2% of the attacks are greater than 5 hours and 1% is greater than 10 hours.

6 Conclusions

In this paper we have seen a technique to estimate denial of service attacks through a passive monitor called "backscatter analysis". Using this technique the authors monitored a /8 network and analyzed packets to detect a variety DoS attacks. Results shows that the size and the length of the attacks are heavytailed, with a small number of long attacks that are part of the overall attack volume.