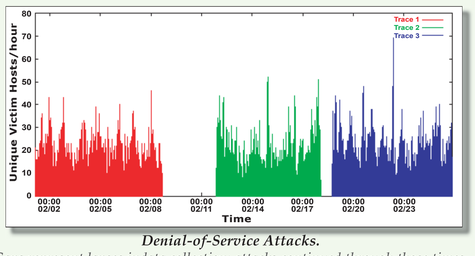
backscatter

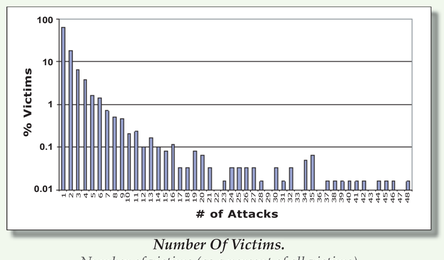
Monitoring Of Global Denial-of-Service Attacks From A Single Location

How Prevalent Are Denial-of-Service (DoS) Attacks?



Denial-of-Service Attacks.
Gaps represent lapses indata collection; attacks continued through those times.

In February, 2000, a series of massive Denial-of-Service attacks incapacitated several high-visibility Internet e-commerce sites, including Yahoo, Ebay, and E*trade. In January, 2001, Microsoft's name server infrastructure was disabled by a similar assault. Attacks of lesser scale occur constantly on the Internet. At least 20 denial-of-service attacks happen every minute of every day.



Number Of Victims.
Number of victims (as a percent of all victims) that were attacked a given number of times.

65% of all victims were attacked once, while 18% were attacked twice and one victim was attacked 48 times.

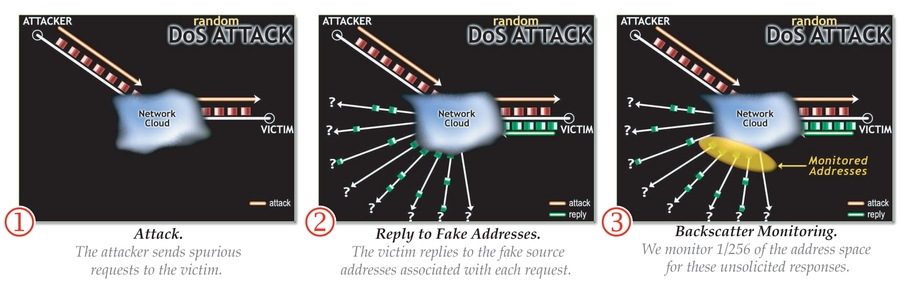
How Can We Detect Denial-of-Service (DoS) Attacks?

Denial-of-Service (DoS) attacks are difficult to monitor. Service and content providers consider data about attacks sensitive and private. Using traditional methods, wide-scale monitoring of DoS attacks requires a tap on a link between the attacker and the victim for every attack. With thousands of attacks occurring every day, the task of obtaining a representative measure of DoS attacks is daunting at best and impossible at worst.

Backscatter analysis is a novel technique that provides quantitative data for a **worldwide view** of DoS activity using only **local monitors**.

The *Backscatter* Method Of Denial-of-Service (DoS) Detection

Denial-of-Service (DoS) attacks often fake the source address of each attacking packet. For many attacks, this forged address is randomly assigned to each packet. However, the victim of the attack doesn't realize that the attacking packets are illegitimate and so the victim answers as many attacking packets as possible. Because the source addresses are faked, the victim sends unsolicited responses to a wide range of IP addresses. By monitoring a large section of the IP address space for these unsolicited responses, we collect a representative measure of the Denial-of-Service attacks that occur at a given point in time. Although we monitor only a portion of the IP address space, we observe all random source Denial-of-Service attacks.



Attack.
The attacker sends spurious requests to the victim.

Reply to Fake Addresses.
The victim replies to the fake source addresses associated with each request.

Backscatter Monitoring.
We monitor 1/256 of the address space for these unsolicited responses.

Fast Facts

In a *single week*, we observed:
4,754 distinct Denial-of-Service attacks
2,385 unique victims
62,233,762 attacking packets

In *three weeks*, we observed:
12,805 distinct Denial-of-Service attacks
6,148 unique victims
191,295,747 attacking packets

More than 20% of all victims are located in Romania or Brazil.

65% of all victims were attacked once, while 18% were attacked twice and one victim was attacked 48 times.

Attacks involved as many as 679,000 packets per second. A rate of 500 packets per second is sufficient to overwhelm a server; 46% of the attacks in each one minute interval had more than 500 packets per second.

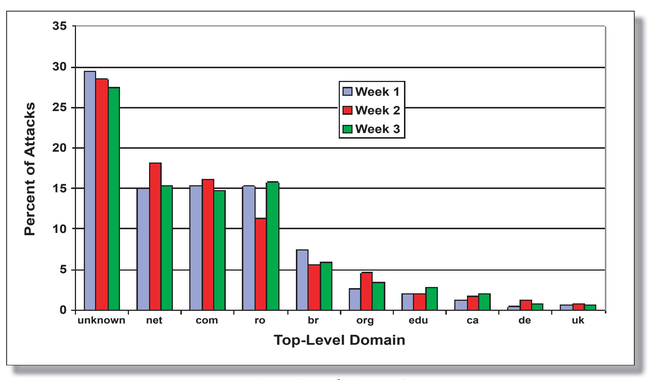
Most Denial-of-Service attacks are relatively short: 50% last less than 10 minutes, 80% last less than 30 minutes, and 90% last less than an hour. However, some attacks span days or weeks.

Researchers

David Moore
dmoore@caida.org
Cooperative Association for Internet Data Analysis
San Diego Supercomputer Center
University of California, San Diego

Geoffrey M Voelker
voelker@cs.ucsd.edu
Department of Computer Science and Engineering
University of California, San Diego

Stefan Savage
savage@cs.ucsd.edu
Department of Computer Science and Engineering
University of California, San Diego



Top-Level Domain.
The percentage of all attacks incurred by each Top-Level Domains.

What Types Of Machines Are Attacked?

Hosts in the .COM and .NET Top-Level Domains (TLDs) incurred approximately 15% of the attacks. .EDU and .ORG were targeted only 2-4% of the time. Romania, a country with relatively poor Internet infrastructure, was targeted nearly as frequently as .NET and .COM, and Brazil was targeted more frequently than .EDU or .ORG. Canada, Germany, and the United Kingdom received 1-2% of all attacks.

IRC Servers were twice as likely to be attacked as webservers, with 2.6% of all attacks. 9.4% of all machines attacked were on broadband links, while 5.7% were dial-up machines. These attacks on home machines suggest that Denial-of-Service attacks are frequently used to wage personal vendettas.

Some Denial-of-Service attacks target network infrastructure. 2-3% target name servers, while 1-3% target routers. This trend is disturbing, since attacking a name server or a router incapacitates ***all*** end hosts who rely on that device for connectivity.

http:// www.ca ida .org/ outreac h/ pape rs/ back sca tter/

cooperative association for internet data analysis ❍ san diego supercomputer center ❍ university of california, san diego
9500 gilman drive, mc0505 ❍ la jolla, ca 92093-0505 ❍ tel. 858-534-5000 ❍ http://www.caida.org/

poster_backscatter_200109

CAIDA is a program of the University of California's San Diego Supercomputer Center (UCSD/SDSC)
Backscatter research is supported by DARPA NGI Cooperative Agreement N66001-98-2-8922, NSF ANIR Grant NCR-9711092 and CAIDA members