Inferring Internet Denial-of-Service Activity

David Moore, Colleen Shannon, Douglas J. Brown, Geoffrey M. Voelker, Stefan Savage

Presented by
Thangam Seenivasan & Rabin Karki
How prevalent are denial-of-service attacks in the Internet?
Why is it important?

Loss could total more than $1.2 billion -analysts

'Bimmense' network assault takes down Yahoo

DDOS attacks have become common

Borrowed from G.Voelkar’s presentation
Recent DDOS attack

Denial-of-Service Attack Knocks Twitter Offline (Updated)

By Eliot Van Buskirk  August 6, 2009 | 10:06 am | Categories: Social Media

Twitter was shut down for hours Thursday morning by what it described as an "ongoing" denial-of-service attack, silencing millions of Tweeters. It was the first major outage the service has suffered in months and possibly the first ever due to sabotage. The outage appeared to begin mid-morning, EST, and affected users around the world. After about three hours, the service was coming
Challenges

• No quantitative data available about the prevalence of DOS attacks
• Obstacles gathering DOS traffic data
  – ISP consider such data private and sensitive
  – Need to monitored from a large number of sites to obtain representative data
Solution

• Backscatter Analysis
  – Estimate prevalence of worldwide DOS attacks
  – Traffic monitoring technique
  – Conservative estimate on the prevalence
  – Lower bound on the intensity of attacks
Outline

- Background
- Methodology
- Attack detection and classification
- Analysis of DOS
DOS attacks

• An attempt to make a computer resource unavailable to its intended users

• Classes of attacks
  – Logic attacks (exploits software flaws)
    • Ping-of-Death
  – Resource attacks
    • Sending a large number of spurious requests

This paper focuses only on resource attacks
Resource attacks

• Network
  – Overwhelm the capacity of network devices
  – Attacker sends packets as rapidly as possible

• CPU
  – Load the CPU by requiring additional processing
  – SYN flood
    • For each SYN packet to a listening TCP port
      – The host must search through existing connections
      – Allocate new data structures
    • Even a small SYN flood can overwhelm a remote host
Distributed attacks

• More powerful attacks
  – From multiple hosts

- Compromised
- Compromised
- Compromised

- Runs a daemon

- Coordinated attack

- Communication for remote control

- Attacker
IP Spoofing

• Many attackers spoof IP source address
  – To conceal their locations
• Use random address spoofing
  – To overcome blacklisting/filtering

This paper focuses solely on attacks with random address spoofing
Outline

• Background
• Methodology
• Attack detection and classification
• Analysis of DOS
Key Idea

• Attackers spoof source address randomly
• Victim, in turn respond to attack packets
• Unsolicited responses (backscatter) equally distributed across IP address space
• Received backscatter is evidence of an attacker elsewhere
Backscattering

Borrowed from G.Voelkar’s presentation
Typical victim responses

<table>
<thead>
<tr>
<th>Packet Sent</th>
<th>Response from Victim</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP SYN (to open port)</td>
<td>TCP SYN/ACK</td>
</tr>
<tr>
<td>TCP SYN (to closed port)</td>
<td>TCP RST (ACK)</td>
</tr>
<tr>
<td>TCP ACK</td>
<td>TCP RST (ACK)</td>
</tr>
<tr>
<td>TCP DATA</td>
<td>TCP RST (ACK)</td>
</tr>
<tr>
<td>TCP RST</td>
<td>TCP RST (ACK)</td>
</tr>
<tr>
<td>TCP NULL</td>
<td>TCP RST (ACK)</td>
</tr>
<tr>
<td>ICMP ECHO Request</td>
<td>no response</td>
</tr>
<tr>
<td>ICMP TS Request</td>
<td>TCP RST (ACK)</td>
</tr>
<tr>
<td>UDP pkt (to open port)</td>
<td>ICMP Echo Reply</td>
</tr>
<tr>
<td>UDP pkt (to closed port)</td>
<td>ICMP TS Reply</td>
</tr>
<tr>
<td>...</td>
<td>protocol dependent</td>
</tr>
<tr>
<td></td>
<td>ICMP Port Unreach</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
</tbody>
</table>
Backscatter Analysis

• Probability of one given host on the Internet receiving at least one unsolicited response during an attack of m packets

\[ 1 - \left(1 - \frac{1}{2^{32}}\right)^m \]

• Probability of n hosts receiving at least one of m packets

\[ 1 - \left(1 - \frac{n}{2^{32}}\right)^m \]
Backscatter Analysis

• Monitor from n distinct hosts
• Expected number of backscatter packets given an attack of m packets

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

• These samples contain
  - Identity of the victim
  - Timestamp
  - Kind of attack
Backscatter Analysis

• If arrival rate of unsolicited packets from a victim is $R'$
• Extrapolated attack rate $R$ on the victim is

$$R \geq R' \frac{2^{32}}{n} \text{ packets per sec}$$
Assumptions

• Address uniformity
  – attackers spoof source addresses at random

• Reliable delivery
  – Attack traffic and backscatter is delivered reliably

• Backscatter hypothesis
  – Unsolicited packets observed by the monitor represent backscatter
Limitation - Address uniformity

• Many attacks do not use address spoofing
  – ISPs increasingly employ ingress filtering

• “Reflector attacks”
  – Source address is specifically selected

• Motivation for IP spoofing has been reduced
  – Automated methods for compromising host
  – DDOS attacks using true IP addresses

Each factor cause the analysis to underestimate the total number of attacks
Limitation – Reliable delivery

- Packets from attacker may be queued and dropped
- Filtered and rate limited by a firewall
- Some traffic do not elicit a response
- Responses may be queued and dropped

Causes the analysis to underestimate the total number of attacks and attack rate
Backscatter hypothesis

• Any server in the Internet can send unsolicited packets
  – Possible to eliminate flows consistently destined to a single host
• Misinterpretation of random port scans as backscatters
• Vast majority attacks can be differentiated from typical scanning activity

Provides a conservative estimate of current denial-of-service activity
Outline

- Background
- Methodology
- Attack detection and classification
- Analysis of DOS
Attack detection and classification

- Identify and extract backscatter packets from raw trace
- Combine related packets into attack flows
  - Based on victims IP address
- Filter out some attack flows based on intensity, duration and rate
Extracting backscatter packets

• Remove packets
  – Involving legitimate hosts
  – Packets that do not correspond to response traffic
  – Remove TCP RST packets used for scanning
    • These scans have sequential scanning patterns
    • Remover RSTs with clearly non-random behavior

• Remove duplicate packets
  – Same <src IP, dst IP, protocol, src port, dst port> in the last five minutes
Flow-based classification

• Flow-based identification
  – Flow: Series of consecutive packets sharing the same victim IP address
  – Flow lifetime: Timeout approach
    • Defines when a flow begins and ends
    • Packets arrive within a fixed timeout relative to the most recent packet in the flow – same flow
    • More conservative timeout: long flows
    • Shorter timeout: large number of short flows
Flow timeout

300 seconds (5 minutes)
Filtering attack flows

• Packet threshold
  – Minimum number of packets necessary to classify it to be an attack
  – Filter out short attacks which have negligible impact

• Attack duration
  – Time between first and last packet of a flow
  – Filter out short attacks

• Packet rate
  – Threshold for maximum rate of packet arrivals
  – Largest packet rate across 1-minute buckets
Packet threshold

![Graph showing number of flows (ccdf) vs. seen backscatter packets. The graph indicates that at 25 packets, the number of flows drops significantly.]
Attack duration

60 seconds
Packet rate

0.5 pps
Extracted Information

- IP Protocol (TCP, UDP, ICMP)
- TCP flag settings (SYN/ACKs, RSTs)
- ICMP payload (copies of original packets)
- Port settings (source and destination ports)
- DNS information
Outline

• Background
• Methodology
• Attack detection and classification
• Analysis of DOS
Analysis: Experimental Platform

Captures all the inbound traffic via Hub

$2^{24}$ distinct IPs, 1/256 of the total IPv4 address space
## Summary of Attack Activity

<table>
<thead>
<tr>
<th>Starting Date</th>
<th>Duration</th>
<th>Attacks</th>
<th>Backscatter Packets</th>
<th>Unique Victim</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>IPs</td>
</tr>
<tr>
<td>2001-02-01</td>
<td>7.5 days</td>
<td>2,618</td>
<td>21,090,742</td>
<td>1,636</td>
</tr>
<tr>
<td>2001-02-11</td>
<td>6.2 days</td>
<td>2,242</td>
<td>30,222,201</td>
<td>1,510</td>
</tr>
<tr>
<td>2001-02-18</td>
<td>7.1 days</td>
<td>2,858</td>
<td>32,159,992</td>
<td>1,921</td>
</tr>
<tr>
<td>2001-02-25</td>
<td>8.9 days</td>
<td>3,346</td>
<td>49,449,404</td>
<td>2,050</td>
</tr>
<tr>
<td>2001-03-06</td>
<td>12.9 days</td>
<td>4,968</td>
<td>59,552,132</td>
<td>2,587</td>
</tr>
<tr>
<td>2001-03-19</td>
<td>8.2 days</td>
<td>2,635</td>
<td>23,588,586</td>
<td>1,618</td>
</tr>
<tr>
<td>2001-04-06</td>
<td>11.8 days</td>
<td>4,343</td>
<td>44,508,551</td>
<td>2,563</td>
</tr>
<tr>
<td>2001-04-22</td>
<td>5.4 days</td>
<td>1,944</td>
<td>14,386,681</td>
<td>1,197</td>
</tr>
<tr>
<td>2001-04-30</td>
<td>6.7 days</td>
<td>828</td>
<td>6,574,228</td>
<td>557</td>
</tr>
<tr>
<td>2001-05-07</td>
<td>14.1 days</td>
<td>4,990</td>
<td>60,647,948</td>
<td>2,933</td>
</tr>
<tr>
<td>2001-05-23</td>
<td>9.1 days</td>
<td>2,993</td>
<td>40,269,047</td>
<td>1,916</td>
</tr>
<tr>
<td>2001-06-01</td>
<td>8.5 days</td>
<td>3,026</td>
<td>47,508,181</td>
<td>1,930</td>
</tr>
<tr>
<td>2001-06-25</td>
<td>8.8 days</td>
<td>2,861</td>
<td>17,408,501</td>
<td>1,897</td>
</tr>
<tr>
<td>2001-07-04</td>
<td>15.8 days</td>
<td>5,666</td>
<td>52,882,496</td>
<td>3,102</td>
</tr>
<tr>
<td>2001-07-19</td>
<td>7.9 days</td>
<td>2,078</td>
<td>36,824,562</td>
<td>1,291</td>
</tr>
<tr>
<td>2001-08-01</td>
<td>7.0 days</td>
<td>974</td>
<td>16,420,358</td>
<td>670</td>
</tr>
<tr>
<td>2001-08-08</td>
<td>6.8 days</td>
<td>1,624</td>
<td>40,248,436</td>
<td>1,059</td>
</tr>
<tr>
<td>2002-05-09</td>
<td>17.5 days</td>
<td>4,820</td>
<td>69,933,861</td>
<td>2,855</td>
</tr>
<tr>
<td>2002-05-29</td>
<td>17.2 days</td>
<td>4,458</td>
<td>103,761,678</td>
<td>2,837</td>
</tr>
<tr>
<td>2002-12-11</td>
<td>7.3 days</td>
<td>2,340</td>
<td>31,139,696</td>
<td>1,016</td>
</tr>
<tr>
<td>2003-11-06</td>
<td>5.0 days</td>
<td>1,416</td>
<td>58,160,582</td>
<td>735</td>
</tr>
<tr>
<td>2004-02-25</td>
<td>10.0 days</td>
<td>5,692</td>
<td>210,181,843</td>
<td>3,088</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>209.9 days</strong></td>
<td><strong>68,720</strong></td>
<td><strong>1,066,919,706</strong></td>
<td><strong>34,725</strong></td>
</tr>
</tbody>
</table>
Summary of Attack Activity

• Collection done over a period of 3 years (Feb 1, 2001 – Feb 25, 2004).
• Captured 22 traces of DoS activity.
• Each trace roughly spans a week.
• Total 68,700 attacks to 34,700 unique victim IPs.
• 1,066 million backscatter packets (≤1/256th of the total backscatter traffic generated)
Summary of Attack Activity

- No strong diurnal patterns, as seen in Web or P2P file sharing.
- Rate of attack doesn’t change significantly over the period of time.
- Attacks were not clustered on particular subnets.
Summary of Attack Activity

- Exhibits daily periodic behavior.
- At the same time everyday, attack increases from est. 2,500 pps to 100,000-160,000 pps.
- Attack persists for one hour before subsiding again.
- Tuesdays off (suggests attacks are scripted).

Fig. 8. The measured intensity of an attack to one particular host during the week of February 18, 2001. The spikes occur at noon local time and last for an hour. The attack skipped February 20, 2001, which was a Tuesday.
## Attack Classification: Protocol

Table IV. Breakdown of Protocols Used in all Attacks Across all Traces. An Entry with Multiple Protocols Indicates an Attack Consisting of a Combination of Packets from Each of the Protocols Listed. “Other” Indicates that the Attack Contained Packets with One or More Miscellaneous Protocols Other Than Those Named in the Table.

<table>
<thead>
<tr>
<th>Kind</th>
<th>Attacks (%)</th>
<th>Packets × 1000 (%)</th>
<th>Victims (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>64,952 (95)</td>
<td>949,373 (89)</td>
<td>32,275 (93)</td>
</tr>
<tr>
<td>ICMP</td>
<td>1,797 (2.6)</td>
<td>24,567 (2.3)</td>
<td>1,334 (3.8)</td>
</tr>
<tr>
<td>TCP/UDP</td>
<td>696 (1.0)</td>
<td>8,526 (0.80)</td>
<td>566 (1.6)</td>
</tr>
<tr>
<td>UDP</td>
<td>466 (0.68)</td>
<td>723 (0.07)</td>
<td>312 (0.90)</td>
</tr>
<tr>
<td>ICMP/TCP</td>
<td>441 (0.64)</td>
<td>63,728 (6.0)</td>
<td>356 (1.0)</td>
</tr>
<tr>
<td>ICMP/IGMP/TCP/UDP</td>
<td>118 (0.17)</td>
<td>342 (0.03)</td>
<td>104 (0.30)</td>
</tr>
<tr>
<td>ICMP/TCP/UDP</td>
<td>87 (0.13)</td>
<td>18,865 (1.8)</td>
<td>64 (0.18)</td>
</tr>
<tr>
<td>IGMP/TCP/UDP</td>
<td>27 (0.04)</td>
<td>42 (0.00)</td>
<td>22 (0.06)</td>
</tr>
<tr>
<td>Other</td>
<td>21 (0.03)</td>
<td>22 (0.00)</td>
<td>10 (0.03)</td>
</tr>
<tr>
<td>Other/TCP</td>
<td>18 (0.03)</td>
<td>62 (0.01)</td>
<td>18 (0.05)</td>
</tr>
<tr>
<td>ICMP/UDP</td>
<td>16 (0.02)</td>
<td>38 (0.00)</td>
<td>15 (0.04)</td>
</tr>
<tr>
<td>ICMP/IGMP/Other/TCP/UDP</td>
<td>16 (0.02)</td>
<td>368 (0.03)</td>
<td>13 (0.04)</td>
</tr>
<tr>
<td>IGMP/Other/TCP/UDP</td>
<td>10 (0.01)</td>
<td>56 (0.01)</td>
<td>8 (0.02)</td>
</tr>
<tr>
<td>IGMP/TCP</td>
<td>9 (0.01)</td>
<td>32 (0.00)</td>
<td>8 (0.02)</td>
</tr>
<tr>
<td>ICMP/IGMP/TCP</td>
<td>7 (0.01)</td>
<td>4 (0.00)</td>
<td>7 (0.02)</td>
</tr>
<tr>
<td>ICMP/Other/TCP</td>
<td>6 (0.01)</td>
<td>13 (0.00)</td>
<td>3 (0.01)</td>
</tr>
<tr>
<td>ICMP/Other</td>
<td>6 (0.01)</td>
<td>3 (0.00)</td>
<td>4 (0.01)</td>
</tr>
<tr>
<td>IGMP/Other/TCP</td>
<td>5 (0.01)</td>
<td>145 (0.01)</td>
<td>5 (0.01)</td>
</tr>
<tr>
<td>Other/TCP/UDP</td>
<td>5 (0.01)</td>
<td>2 (0.00)</td>
<td>5 (0.01)</td>
</tr>
<tr>
<td>IGMP/Other</td>
<td>5 (0.01)</td>
<td>3 (0.00)</td>
<td>4 (0.01)</td>
</tr>
</tbody>
</table>
Table shows –

• 95% of attacks and 89% of packets use TCP protocol.
• Distant second is ICMP with 2.6% of attacks.
• Breakdown of TCP attacks shows most of the attacks target multiple ports.
• Most popular individual target ports: HTTP (80), IRC (6667), port 0, Authd(113)
Attack Classification: Rate

• 500 SYN pps are enough to overwhelm a server.
• 65% attacks had 500 pps or higher.
• 4% attacks had ≥ 14,000 pps, enough to compromise attack-resistant firewalls.
Attack Classification: Duration

- 60% attacks less than 10 min
- 80% are less than 30 min
- 2.4% are greater than 5 hrs
- 1.5% are greater than 10 hrs
- 0.53% span multiple days
- PDF graph shows peak is at 5 min (10.8%), 10 min (9.7%)

Fig. 10. Cumulative and probability distributions of attack durations.
Victim Classification: Type

Table VI. Breakdown of Victim Hostnames

<table>
<thead>
<tr>
<th>Kind</th>
<th>Attacks (%)</th>
<th>Packets × 1000 (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-Addr Arpa</td>
<td>28,547 (42)</td>
<td>498,775 (47)</td>
</tr>
<tr>
<td>Unclassified</td>
<td>25,216 (37)</td>
<td>404,111 (38)</td>
</tr>
<tr>
<td>Broadband</td>
<td>5,520 (8.0)</td>
<td>31,006 (2.9)</td>
</tr>
<tr>
<td>Dial-Up</td>
<td>4,864 (7.1)</td>
<td>39,479 (3.7)</td>
</tr>
<tr>
<td>IRC Server</td>
<td>1,156 (1.7)</td>
<td>49,950 (4.7)</td>
</tr>
<tr>
<td>Nameserver</td>
<td>1,141 (1.7)</td>
<td>17,685 (1.7)</td>
</tr>
<tr>
<td>Web Server</td>
<td>996 (1.4)</td>
<td>11,968 (1.1)</td>
</tr>
<tr>
<td>Router</td>
<td>885 (1.3)</td>
<td>11,148 (1.0)</td>
</tr>
<tr>
<td>Mail Server</td>
<td>377 (0.55)</td>
<td>2,501 (0.23)</td>
</tr>
<tr>
<td>Firewall</td>
<td>18 (0.03)</td>
<td>297 (0.03)</td>
</tr>
</tbody>
</table>
Victim Classification: TLD

Table VII. Breakdown of Victim Top-Level Domains (TLDs). The “arpa” TLD represents those attacks for which a reverse DNS lookup failed on the victim IP address.

<table>
<thead>
<tr>
<th>Kind</th>
<th>Attacks (%)</th>
<th>Packets×1000 (%)</th>
<th>Victims (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>arpa</td>
<td>28,547 (42)</td>
<td>498,775 (47)</td>
<td>14,513 (42)</td>
</tr>
<tr>
<td>net</td>
<td>9,291 (14)</td>
<td>150,339 (14)</td>
<td>5,113 (15)</td>
</tr>
<tr>
<td>com</td>
<td>7,721 (11)</td>
<td>162,539 (15)</td>
<td>4,046 (12)</td>
</tr>
<tr>
<td></td>
<td>7,235 (11)</td>
<td>33,661 (3.2)</td>
<td>3,031 (8.7)</td>
</tr>
<tr>
<td>edu</td>
<td>2,822 (4.1)</td>
<td>22,286 (2.1)</td>
<td>1,228 (3.5)</td>
</tr>
<tr>
<td></td>
<td>1,219 (1.8)</td>
<td>13,258 (1.2)</td>
<td>659 (1.9)</td>
</tr>
<tr>
<td></td>
<td>1,167 (1.7)</td>
<td>5,307 (0.50)</td>
<td>636 (1.8)</td>
</tr>
<tr>
<td>org</td>
<td>890 (1.3)</td>
<td>26,340 (2.5)</td>
<td>431 (1.2)</td>
</tr>
<tr>
<td></td>
<td>638 (0.93)</td>
<td>5,843 (0.55)</td>
<td>424 (1.2)</td>
</tr>
<tr>
<td></td>
<td>610 (0.89)</td>
<td>1,793 (0.17)</td>
<td>375 (1.1)</td>
</tr>
<tr>
<td></td>
<td>566 (0.82)</td>
<td>1,857 (0.17)</td>
<td>306 (0.88)</td>
</tr>
<tr>
<td></td>
<td>520 (0.76)</td>
<td>14,467 (1.4)</td>
<td>154 (0.44)</td>
</tr>
<tr>
<td></td>
<td>435 (0.63)</td>
<td>3,114 (0.29)</td>
<td>247 (0.71)</td>
</tr>
<tr>
<td></td>
<td>429 (0.62)</td>
<td>4,422 (0.41)</td>
<td>220 (0.63)</td>
</tr>
<tr>
<td></td>
<td>409 (0.60)</td>
<td>3,510 (0.33)</td>
<td>221 (0.64)</td>
</tr>
<tr>
<td></td>
<td>405 (0.59)</td>
<td>1,516 (0.14)</td>
<td>177 (0.51)</td>
</tr>
<tr>
<td></td>
<td>383 (0.56)</td>
<td>1,794 (0.17)</td>
<td>188 (0.54)</td>
</tr>
<tr>
<td></td>
<td>378 (0.55)</td>
<td>7,710 (0.72)</td>
<td>244 (0.70)</td>
</tr>
<tr>
<td></td>
<td>346 (0.50)</td>
<td>11,548 (1.1)</td>
<td>216 (0.62)</td>
</tr>
<tr>
<td></td>
<td>313 (0.46)</td>
<td>1,083 (0.10)</td>
<td>145 (0.42)</td>
</tr>
</tbody>
</table>

- Over 10% targeted com & net
- 1.3-1.7% targeted org & edu
- 11% were targeted to ro
- 4% to br
Victim Classification: Repeated Attacks

- Most victims (89%) were attacked in only one trace.
- Most of the remaining victims (7.8%) appear in two traces.
- Victims can appear in multiple traces because of attacks that span trace boundaries.
- 3% victims appear in more than 3 traces, nevertheless.
Victim Classification: Repeated Attacks

(b) CCDF showing the length of time between the first and last traces in which we observed an attack targeting a victim. Only victims attacked in more than one trace are shown.

15 victims that appear in 10 or more traces
Validation

• Nearly all of the packets attribute to the backscatter do not provoke a response, so these packets could not have been used to probe the monitored network.

• Anderson-Darling test (a statistical test of whether there is evidence that a given sample of data did not arise from a given probability distribution) to determine if the distribution of destination addresses is uniform. Validated for most attacks at the 0.05 significance level.
Validation cont’d…

• Duplicated portion of the analysis using data taken from several university-related networks in California.
  – Although this is a much smaller dataset; for 98% of the victim IP recorded in this dataset, corresponding record was found at the same time in larger dataset.

• Data from Asta Networks describing DoS attacks detected also qualitatively confirms the data in this paper.
Conclusions

• Presented new technique called “backscatter analysis” for estimating DoS attack activity on the Internet.
• Observed widespread DoS attacks distributed among many domains and ISPs.
• Size and length of attacks were heavy tailed.
• Surprising number of attacks directed at a few foreign countries. (or as we non-US citizens call them – home countries).
• Witnessed over 68,000 attacks during 3 years, with little signs of abatement.
Questions?