Inferring Internet Denial-of-Service Activity

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

Presented by Qian HE (Steve)
CS 577 – Prof. Bob Kinicki

How prevalent are
DoS attacks
in the Internet?

Agenda

- Introduction
- Background
- Methodology
- Attack Detection and Classification
- Analysis of Denial-Of-Service Activity
- Conclusion

Agenda

- Introduction
- Background
- Methodology
- Attack Detection and Classification
- Analysis of Denial-Of-Service Activity
- Conclusion

Introduction - Examples

"2,000–3,000 active denial-of-service attacks per week"
"68,700 attacks on over 34,700 distinct Internet hosts belonging to more than 5,300 distinct organizations"

- Feb 2000, Yahoo, Ebay, and E*trade.
- Jan 2001, Microsoft's name server.
- 2002, root DNS servers.
- Late 2003, SCO's corporate Website.

Introduction - Motivation

- Many of the attacks are motivated by mischief or spite, others are likely born out of religious, ethnic or political tensions, and still others have been clearly focused around commercial gain.

Introduction - Problems

- There is little quantitative data about the prevalence of these attacks nor any representative characterization of their behavior.
- Obstacles hampering the collection of an authoritative DoS traffic dataset:
  - ISPs consider such data sensitive and private
  - Measuring Internet-wide attacks presents a significant logistical challenge.

Agenda

- Introduction
- Background
- Methodology
- Attack Detection and Classification
- Analysis of Denial-Of-Service Activity
- Conclusion

Background - Attack Types

- There are two principal classes of attacks:
  - Logic Attacks
  - Resource Attacks (this paper focuses solely on)

Background - Resource Attacks

- Related consequences:
  - Overwhelm the capacity of intervening network devices.
  - Overwhelm the capacity of CPU.

Background - IP Spoofing

- Spoof the IP source address of each packet the attacker send
- This paper focuses solely on attacks using random address spoofing

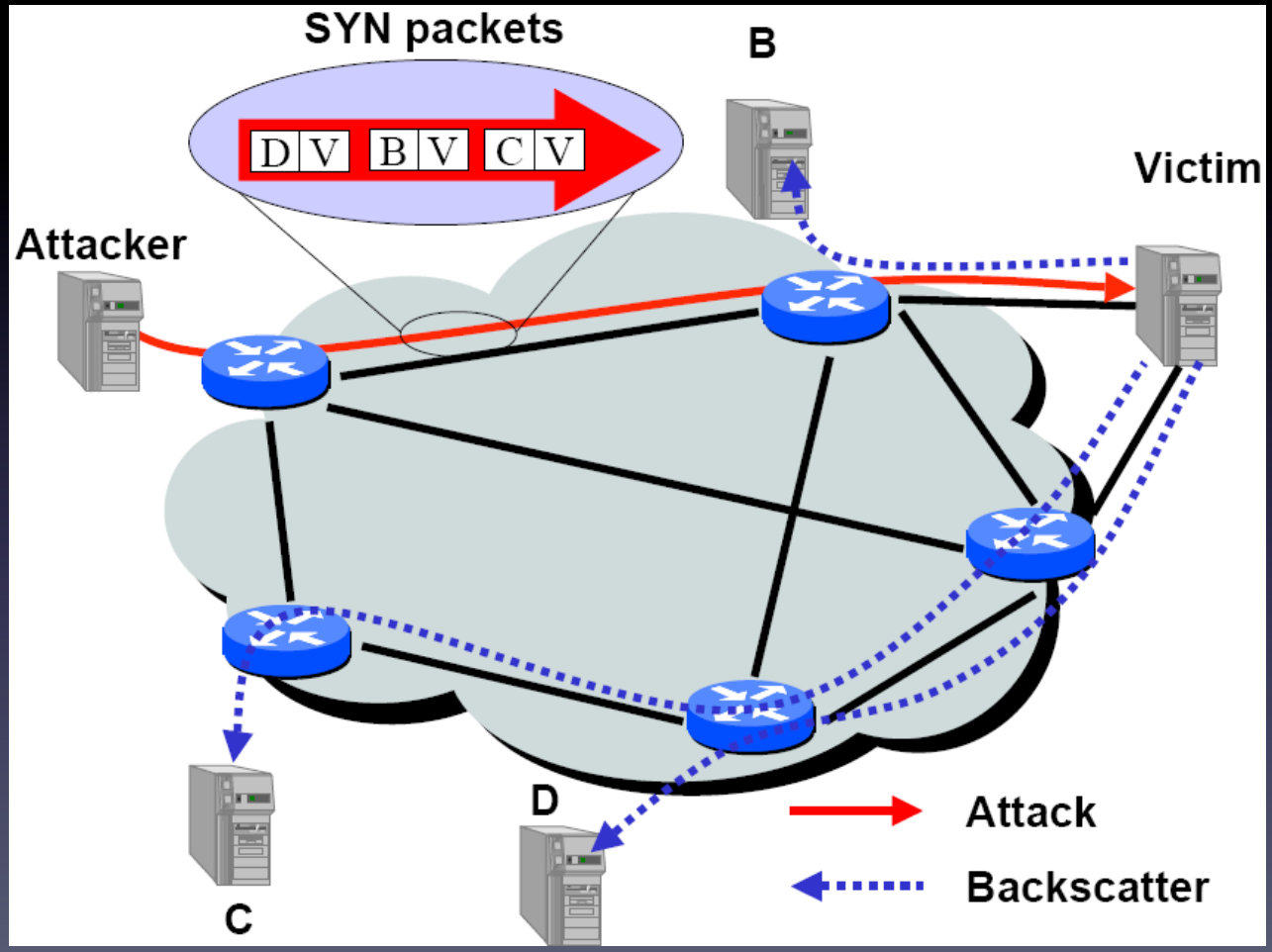
Agenda

- Introduction
- Background
- Methodology
- Attack Detection and Classification
- Analysis of Denial-Of-Service Activity
- Conclusion

Methodology - Ideas

- Attacker's source address is selected at random.
- Victim's responses are also distributed across the entire Internet address space.

Methodology - Backscatter



Borrowed from Geoffrey M. Voelker's Presentation

Methodology - Backscatter Analysis

- During an attack of m packets, the p of 1 given host receiving at least 1 unsolicited response from the victim is

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

- If 1 monitors n distinct IP addresses, then the expected p of observing at least 1 packet from the attack is

$$1-\left(1-\frac{n}{2^{32}}\right)^{m}$$

Methodology - Backscatter Analysis

- The expected number of unsolicited responses seen during an attack of m packets at a single host is

$$\frac{m}{2^{32}}$$

- The expected number of monitoring n distinct IP addresses, the responses seen is

$$\frac{nm}{2^{32}}$$

Methodology - Backscatter Analysis

- Use the average arrival rate of unsolicited responses directed at the monitored address range to estimate the actual rate of the attack being directed at the victim:

$$R \geq R' \cdot \frac{2^{32}}{n}$$

Methodology - Analysis Limitations

- Address uniformity: attackers spoof source addresses at random.
- Reliable delivery: attack traffic is delivered reliably to the victim and backscatter is delivered reliably to the monitor.
- Backscatter hypothesis: unsolicited packets observed by the monitor represent backscatter.

Methodology - Analysis Limitations

- Address Uniformity
  - Many attacks today do not use address spoofing at all.
  - "Reflector attacks" pose a second problem for source address uniformity.
  - Motivation for address spoofing has been reduced.

Methodology - Analysis Limitations

- Reliable Delivery
  - Packets may be queued and dropped.
    - from the attacker
    - from victim
  - Packets may be filtered or rate-limited by firewall or intrusion detection software.
  - Some forms of attack traffic (e.g. TCP RST messages) do not typically elicit a response.

Methodology - Analysis Limitations

- Backscatter Hypothesis
  - Any server in the Internet is free to send unsolicited packets.
  - Misinterpretation of random port scans as backscatter
  - Vast majority of attacks can be trivially differentiated from typical scanning activity.

Methodology

"In spite of its limitations, we believe our overall approach is sound and provides at worst a conservative estimate of current denial-of-service activity. " – this paper

Agenda

- Introduction
- Background
- Methodology
- Attack Detection and Classification
- Analysis of Denial-Of-Service Activity
- Conclusion

Attack Detection and Classification

- Extracting Backscatter Packets
- Flow-Based Classification
  - Flow-Based Identification
  - Flow Timeout
- Deriving Denial-of-Service Attacks
  - Packet Threshold
  - Attack Duration
  - Packet Rate
- Extracted Information

Extracting Backscatter Packets

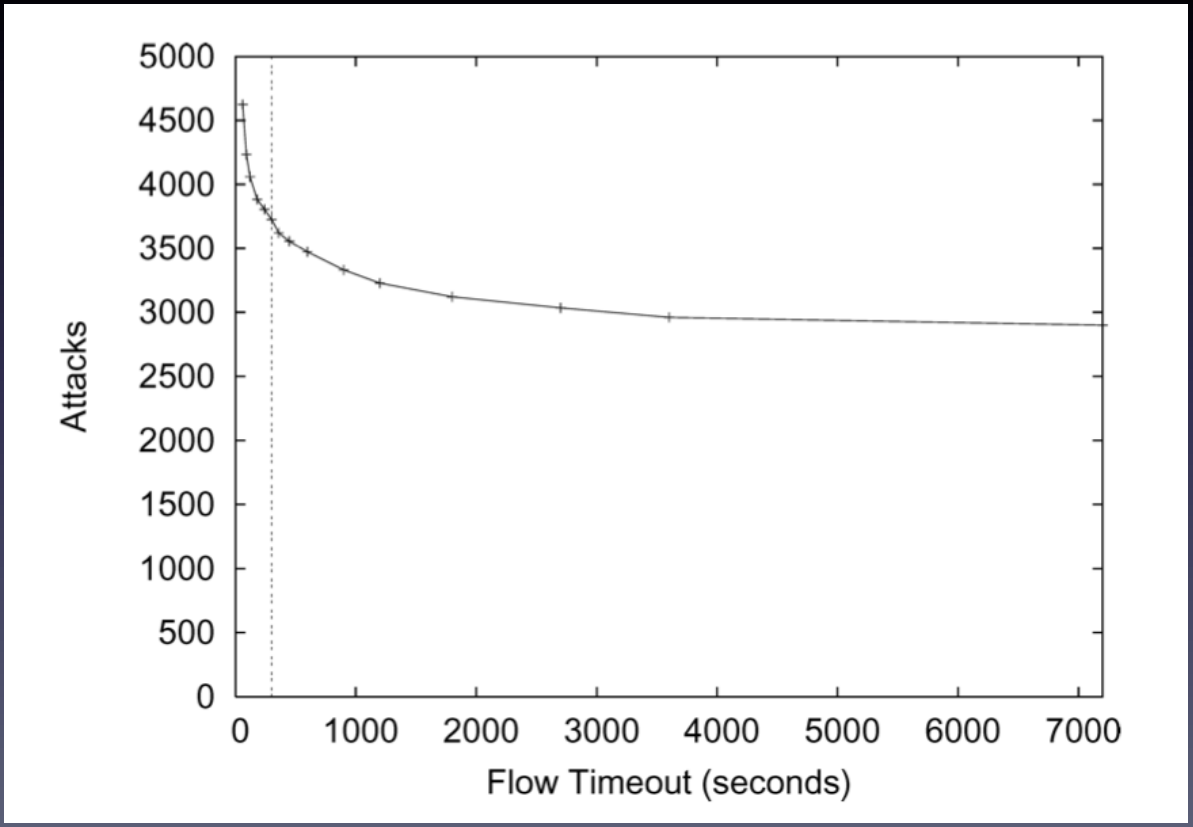
- Remove
  - packets involving legitimate hosts
  - packets that do not correspond to response traffic
  - traffic from hosts that use TCP RST packets for scanning
  - duplicate packet with the same flow tuple <source IP address, destination IP ad- dress, protocol, source port, destination port> in the last five minutes

Flow-Based Classification

- Flow-Based Identification
  - Flow is a series of consecutive packets sharing the same victim IP address.
  - The first packet seen for a victim creates a new flow.
  - If the packets arrive at the telescope from that victim within a fixed timeout relative to the most recent packet in this flow, we associate these packets with that flow.

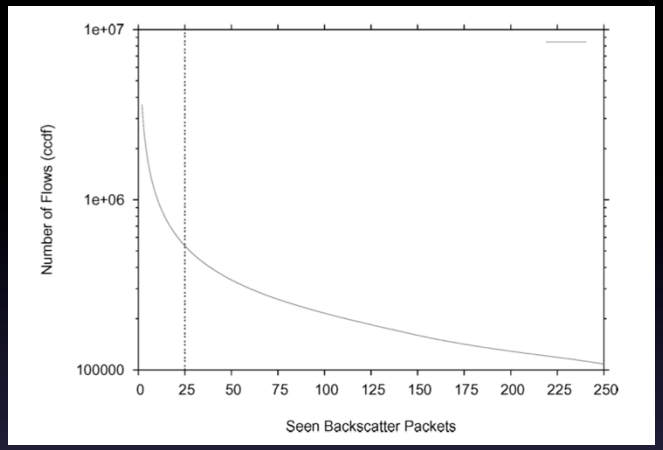
Flow-Based Classification

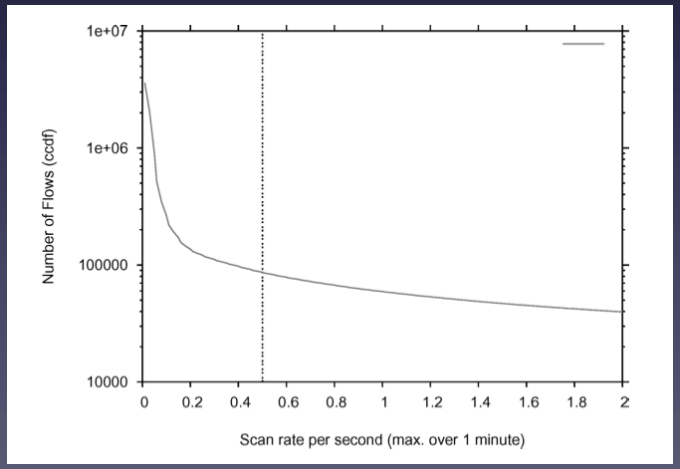
- Flow Timeout (5 minutes)

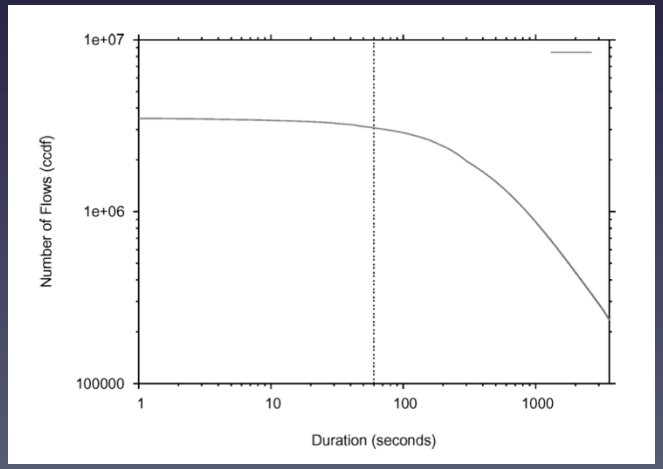


Deriving Denial-of-Service Attacks

- Packet Threshold (> 25 packets)
- Attack Duration (> 60 seconds)
- Packet Rate (> 0.5 pps)







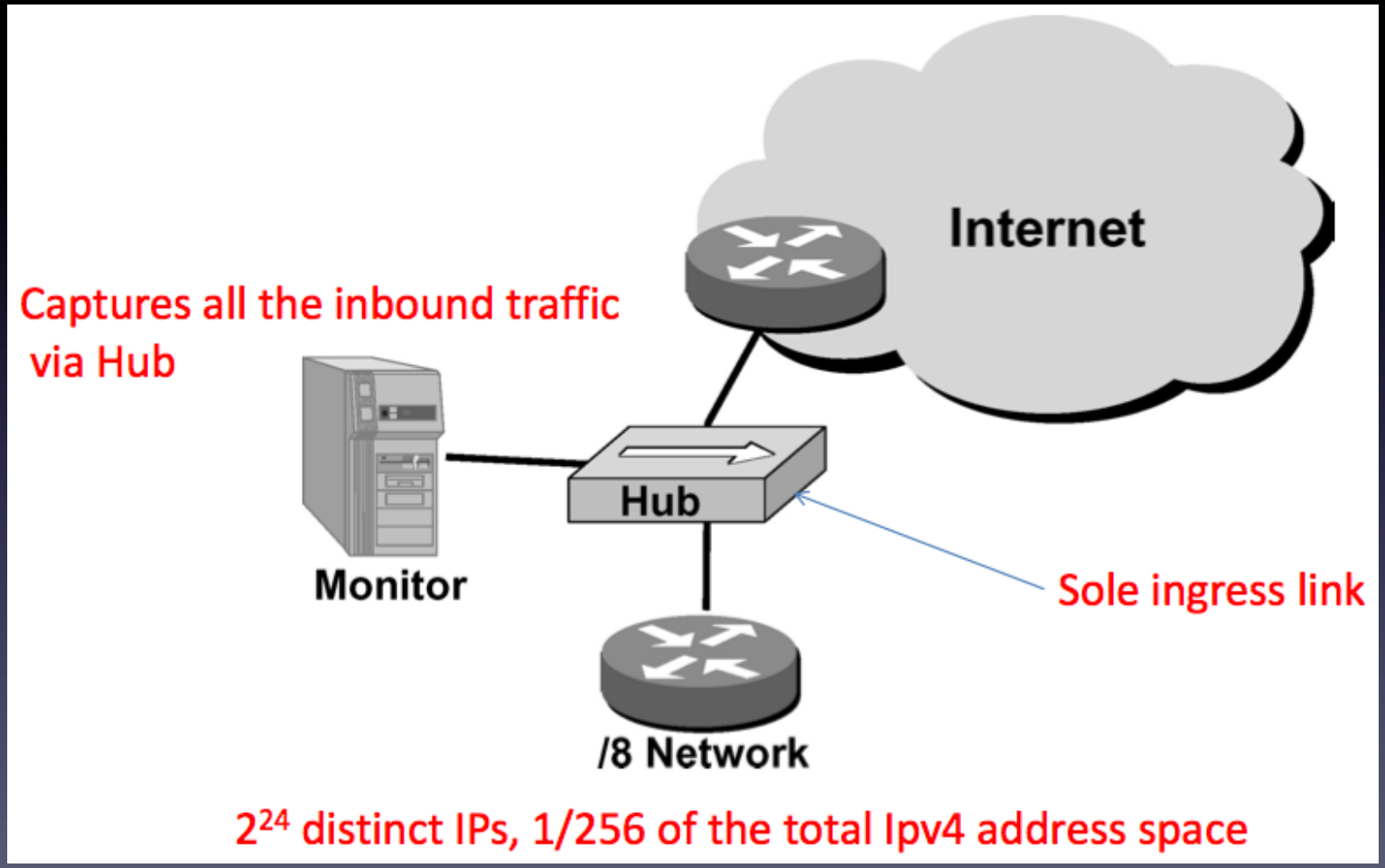
Extracted Information

- IP protocol
- TCP flag settings
- ICMP payload (copies of the original packet)
- Port settings
- DNS information (source address, the victim).

Agenda

- Introduction
- Background
- Methodology
- Attack Detection and Classification
- Analysis of Denial-Of-Service Activity
- Conclusion

Analysis of Denial-Of-Service Activity



Borrowed from Thangam Seenivasan & Rabin Karki's Presentation

Summary of Attack Activity

- From 02/01/2001 to 02/25/2004
- 22 traces of DoS activity
- Each trace roughly spans one week
- 68,700 attacks to 34,700 unique victim IP addresses in 5,300 distinct DNS domains
- 1,066 million backscatter packets (less than 1/256 of the backscatter traffic)

Interesting Features

- No strong diurnal patterns.
- Rate of attack doesn't change significantly over the period of time.
- Attacks were not clustered on particular subnets.
- 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).

Attack Classification

- Attack Protocols
  - The vast majority of attacks (93%) and packets (88%) use TCP
  - 2.6% used ICMP
  - Most popular services targeted are HTTP (port 80), IRC (6667), port 0, and Authd (113)
- Attack Rate
  - 500 SYN pps is enough to overwhelm a server
  - 65% of attacks had an estimated rate of this rate or higher
  - A server can be disabled by a flood of 14,000 pps
  - 4% of attacks would compromise these attack-resistant firewalls
- Attack Duration
  - 60% attacks less than 10 min
  - 80% are less than 30 min
  - 85% last less than 1 hr
  - 2.4% are greater than 5 hrs
  - 1.5% are greater than **10 hrs**
  - 0.53% span **multiple days**

Victim Classification

- Victim Type
- Top-Level Domains
- Victims of Repeated Attacks

Victim Type

- roughly half of the victims are broadband users
- slightly less than 10% are dial-up
- 5–10% of the victims are located on educational networks
- a small number of victims appear to be Internet hosting centers
- the majority of victims of the attacks are home users and small businesses
- a significant number of attacks against victims running IRC
- many reverse DNS mappings have been clearly compromised by attackers (e.g. "is.on.the.net.illegal.ly").
- a small but significant fraction of attacks directed against network infrastructure
- Over 1.3% of attacks target routers
- 1.7% target name servers

Top-Level Domains

- over 10% of the attacks targeted the .com and .net TLDs
- fewer attacks (1.3–1.7%) targeted the .edu and .org domains
- a disproportionate concentration of attacks to a small group of countries
- attackers targeted Romania (.ro) as frequently as .net and .com
- attackers targeted Brazil (.br) more than .edu and .org combined.

Victims of Repeated Attacks

- most victims (89%) were attacked in only one trace (typically spanning roughly one week)
- most of the remaining victims (7.8%) appear in two traces
- victims can appear in multiple traces because of attacks that span trace boundaries
- 74% of the victims in each trace were targeted only during the collection of that trace
- a small percentage of victims (3%) appear in more than three traces

Trace: attack that covers a week or more)

Validation

- Nearly all of the packets are attributed to backscatter that does not itself provoke a response (e.g. TCP RST, ICMP Host Unreachable)
- Distribution of destination addresses is consistent with a uniform distribution at the 0.05 significance level.
- Data from several university-related networks in Northern California and Asta Networks qualitatively confirmed it.

Conclusion

- presented a new technique, "backscatter analysis," for estimating DoS attack activity in the Internet
- observed widespread DoS attacks in the Internet
- witnessed over 68,000 attacks
- the size and length of the attacks were heavy-tailed
- a surprising number of attacks directed at a few foreign countries, at home machines, and towards particular Internet services

Thanks

Q & A