Inferring Internet Denial-of-Service Activity

Alec Buchanan
Jason Lawrence

Agenda

1. Intro
2. Background - Underlying Mechanisms of Denial of Service Attack
3. Backscatter Technique
4. Attack Classifying
5. Experimental Platform
6. Results
7. Discussion

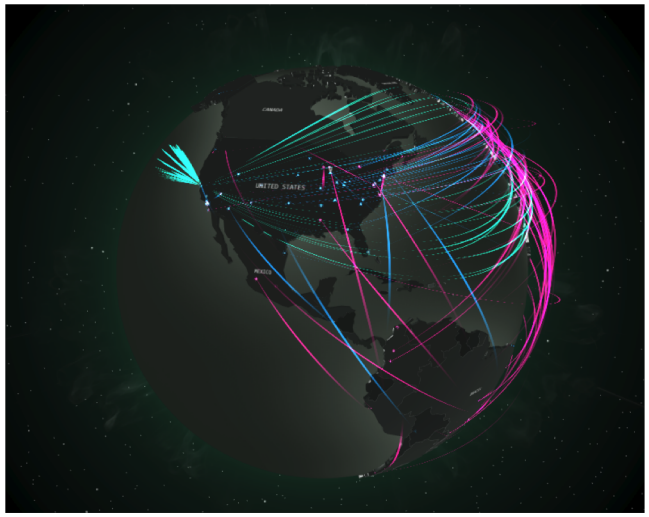
Intro

1. Goal
2. Motivation
3. Accomplishments

Goal

“Determine how prevalent denial-of-service attacks are in the Internet today”

- Understand current threats
- Enable long term analyses of trends



Motivation

- Little available data on DoS attack occurrences
- Poor understanding of the nature of today’s threats

Accomplishments

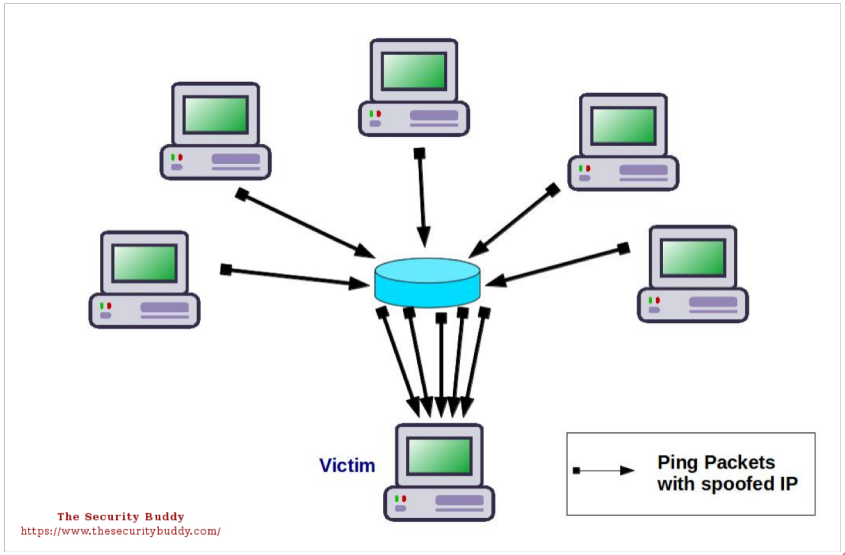
- The only publically available data on DoS activity
- Better understanding of the nature of today’s threats
- Baseline for longer-term comparison and analysis

Underlying Mechanisms of Denial of Service Attack

1. DoS Attacks
2. Flood Attacks
3. Distributed Denial of Service
4. IP Spoofing
5. Denial of Service with IP Spoofing

DoS Attacks

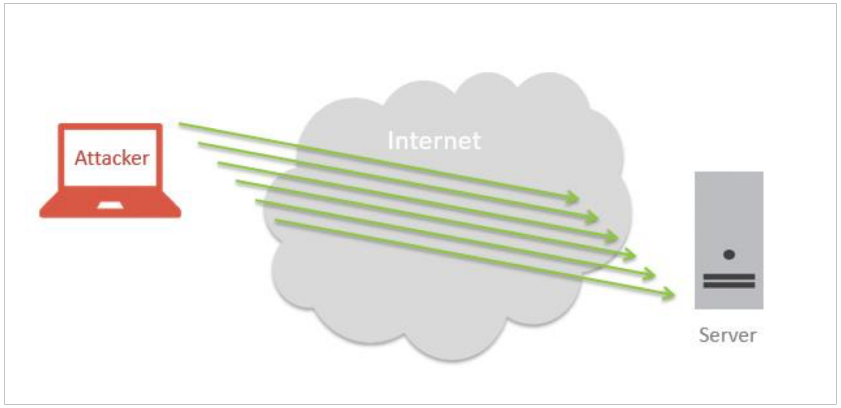
- Consumes resources of a host or network
- Two main types:
  - Logic Attacks
  - Flood Attacks



DoS: Flood Attack

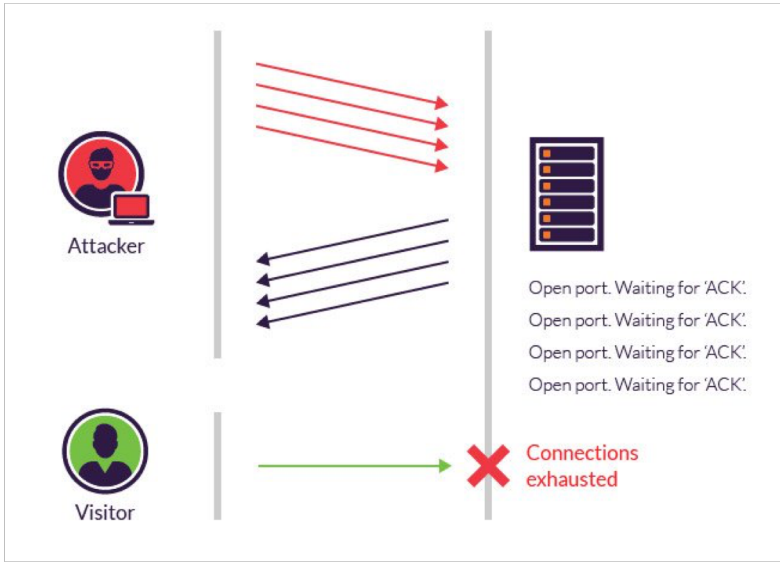
Goal: focus on overwhelming resources (CPU, Memory, Network)

- Sends large number of requests (flood)
- Hard to defend against
- All work here refers to flooding attacks



DoS: Flood Attack Examples

- TCP SYN
- TCP ACK
- NUL
- RST
- DATA

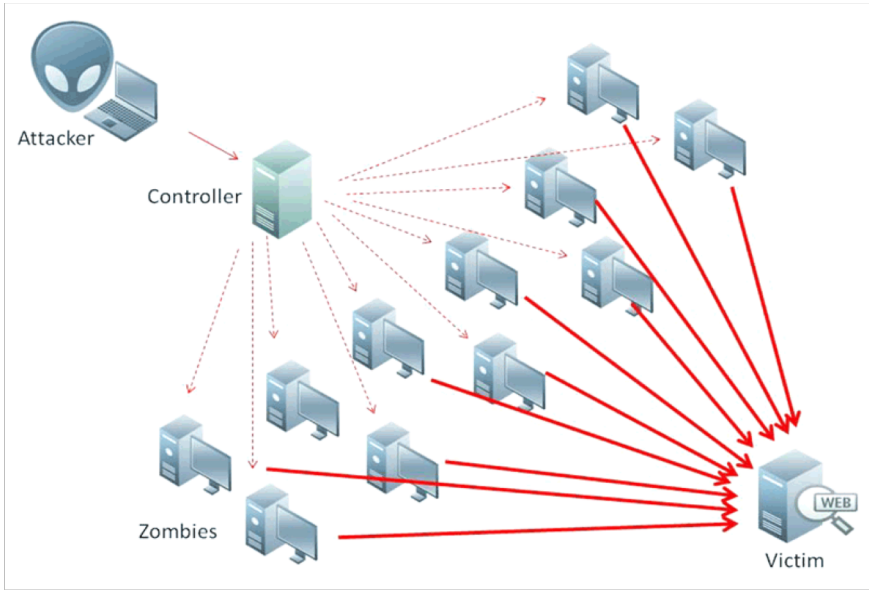


Packet sent	Response from victim
TCP SYN (to open port)	TCP SYN/ACK
TCP SYN (to closed port)	TCP RST (ACK)
TCP ACK	TCP RST (ACK)
TCP DATA	TCP RST (ACK)
TCP RST	no response
TCP NULL	TCP RST (ACK)
ICMP ECHO Request	ICMP Echo Reply
ICMP TS Request	ICMP TS Reply
UDP pkt (to open port)	protocol dependent
UDP pkt (to closed port)	ICMP Port Unreach
...	...

Table 1: A sample of victim responses to typical attacks.

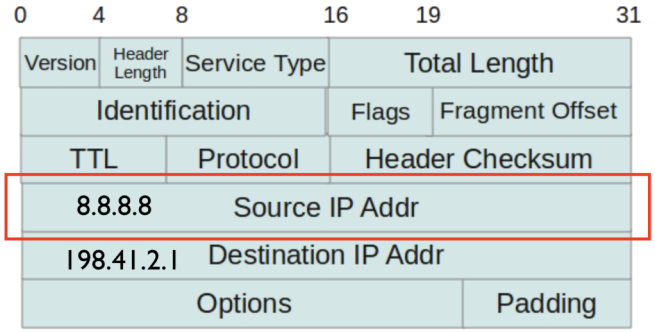
Distributed Denial of Service

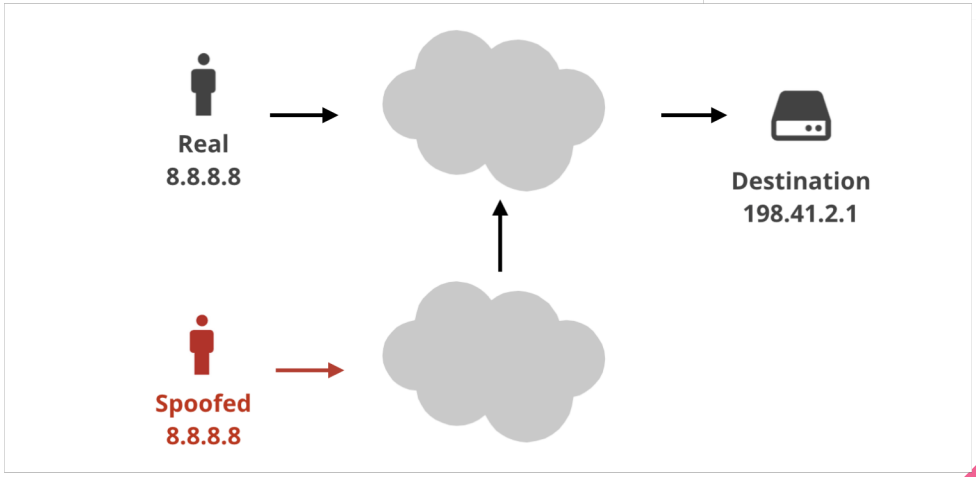
- Uses a network of bots
- Enables attacker to send more packets



IP Spoofing

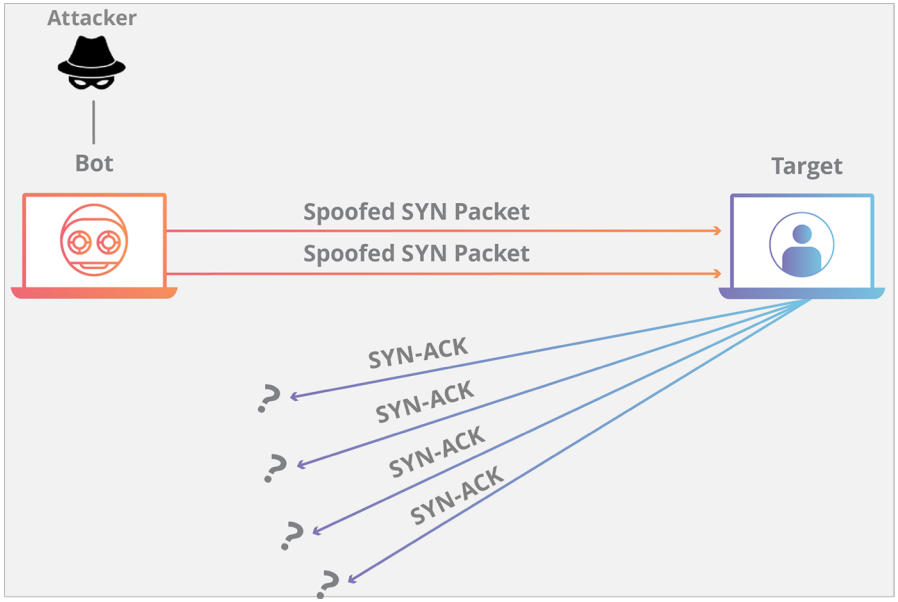
- TCP does not verify source address
- Anyone can spoof a packet's source address





IP Spoofing and DoS

- IP source addresses are typically spoofed
- Conceals the sender's identity
- Victim responds to spoofed address

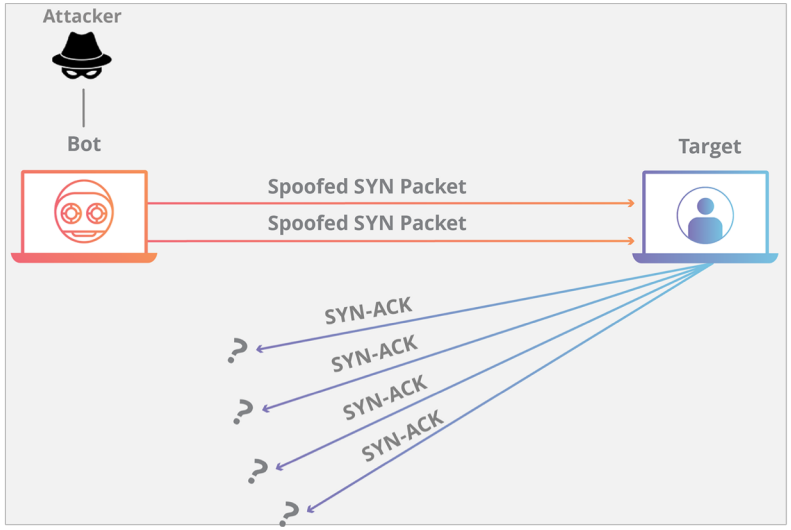


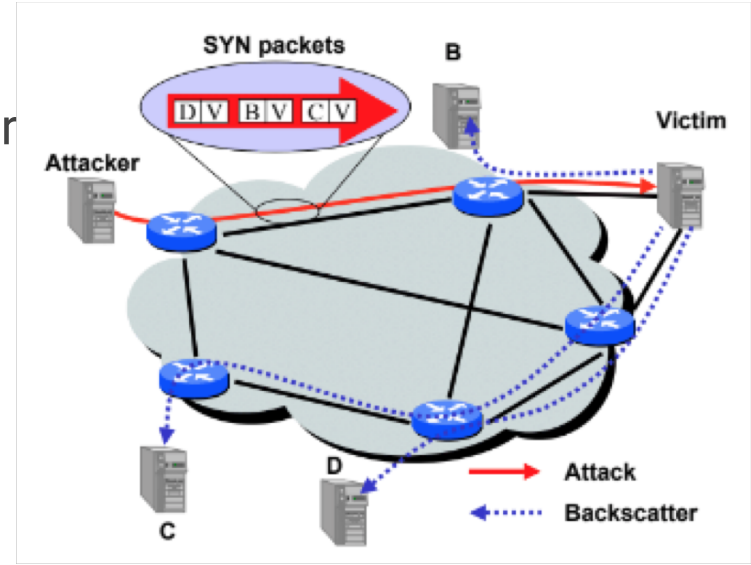
Backscatter Technique

1. What is Backscatter
2. Backscatter Assumptions
3. Backscatter Capturing
4. Backscatter Analysis
5. Backscatter Bias

Backscatter

- Result of DoS attack with spoofed source addr
- Victim sends responses source address
- Responses are sent all over the internet
  - This is called backscatter





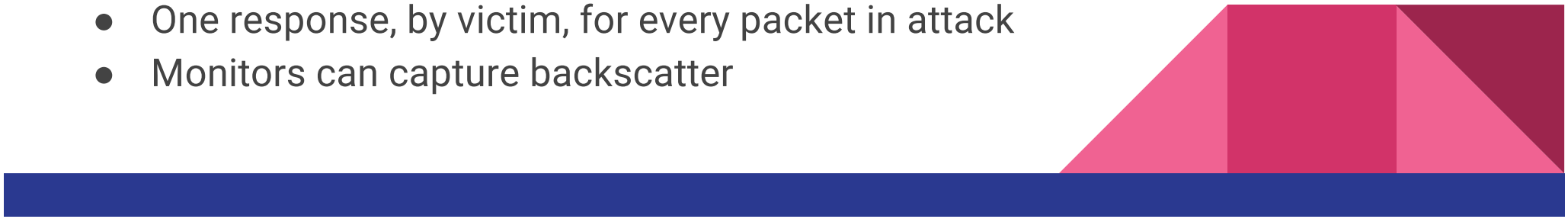
Backscatter Analysis Assumptions

Main Assumptions

1. Address Uniformity: Per-packet random source addresses
2. Reliable Delivery: No packets are dropped
3. Backscatter Hypothesis: Unsolicited packets are considered backscatter

Secondary Assumptions

- One response, by victim, for every packet in attack
- Monitors can capture backscatter



Backscatter Capturing

- Backscatter must be captured to detect DoS attack
- Monitors listen for backscatter
- Observe large enough sample for effective detection

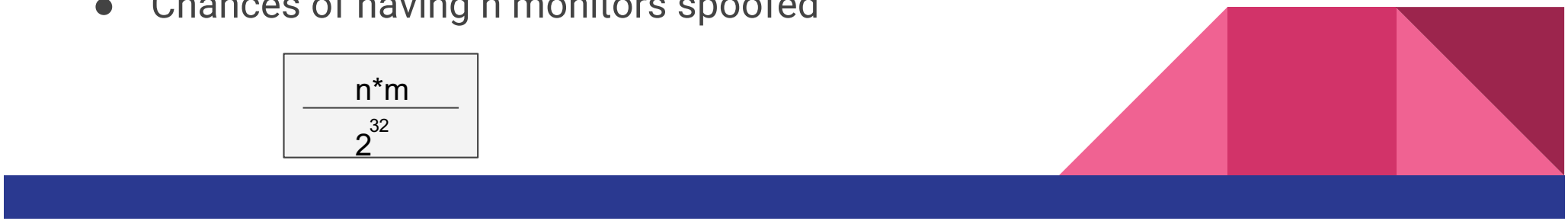
Probability

- Chances of having one monitor's IP spoofed

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

- Chances of having n monitors spoofed

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



Backscatter Analysis

Metrics

- Victim identity
- Type of attack
- Timestamp
- Average arrival rate

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

Packet sent	Response from victim
TCP SYN (to open port)	TCP SYN/ACK
TCP SYN (to closed port)	TCP RST (ACK)
TCP ACK	TCP RST (ACK)
TCP DATA	TCP RST (ACK)
TCP RST	no response
TCP NULL	TCP RST (ACK)
ICMP ECHO Request	ICMP Echo Reply
ICMP TS Request	ICMP TS Reply
UDP pkt (to open port)	protocol dependent
UDP pkt (to closed port)	ICMP Port Unreach
...	...

Table 1: A sample of victim responses to typical attacks.

Backscatter Accuracy/Biases

- Ingress Filtering
- Reflector Attacks
- Source Address Distribution
- Reliable Packet Delivery and Response
- Unsolicited Responses

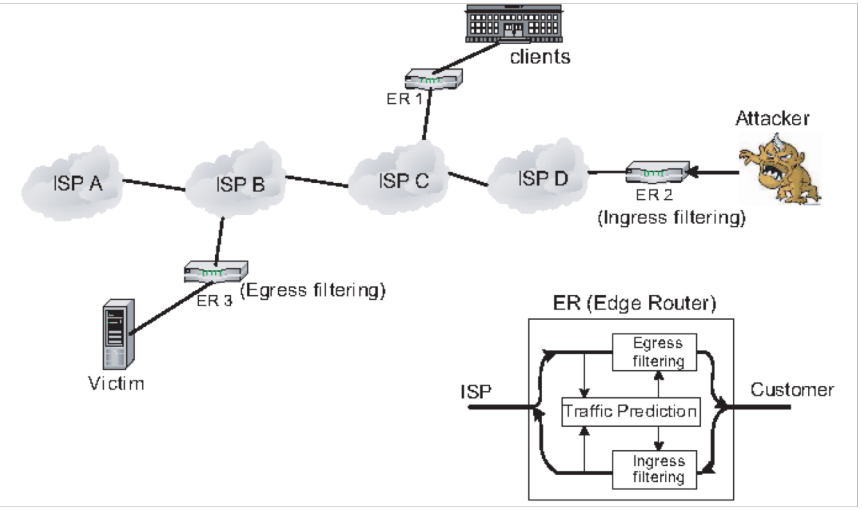
Backscatter Bias: Ingress Filtering

What Is Ingress Filtering

- Deployed by ISP
- Filters out spoofed packets

Effect On Backscatter

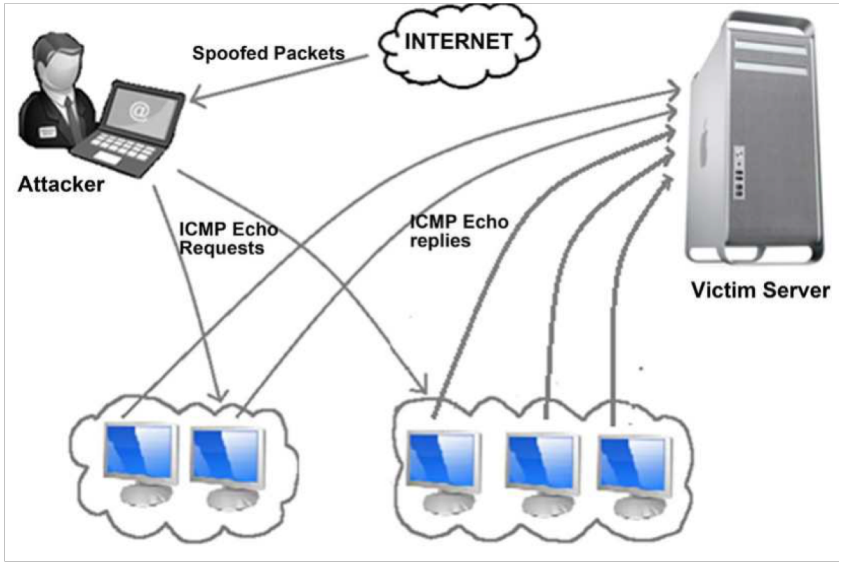
- Packets could be dropped
- Harder to detect DoS attempt



Backscatter Bias: Reflector Attacks

Reflector Attacks

- Example: Smurf Attack
- Destination and spoofed source address are essential for the attack



Backscatter and Reflector Attacks

- No backscatter generated from reflector attacks
- Monitor must be picked as the innocent third party

Backscatter Bias: Source Address Distribution

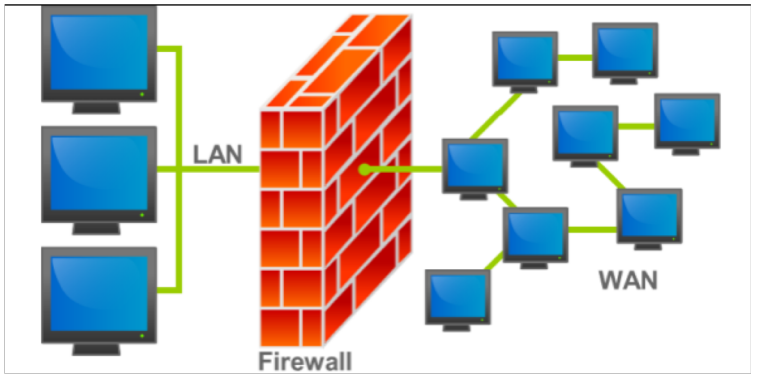
Assumption: Source addresses are randomly chosen

- Backscatter capturing needs randomly spoofed sources
- Monitor must a spoofed source

Backscatter Bias: Reliable Packet Delivery and Response

Assumption: Packets are delivered reliably

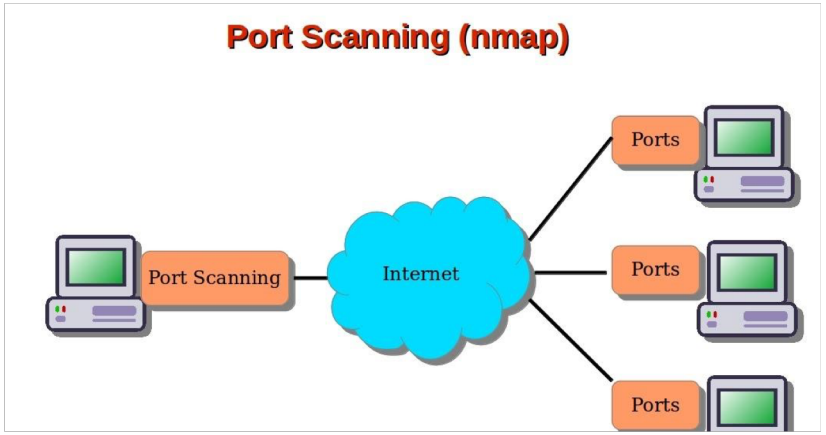
- Packets not always delivered reliably
- Packets dropped for various reasons
  - Firewalls
  - Intrusion detection software
  - Poor connections



Backscatter Bias: Unsolicited Responses

Assumption: Backscatter Hypothesis

- Easy to misinterpret noise
- Anyone can send unsolicited packets
  - Port scans
  - Random backscatter



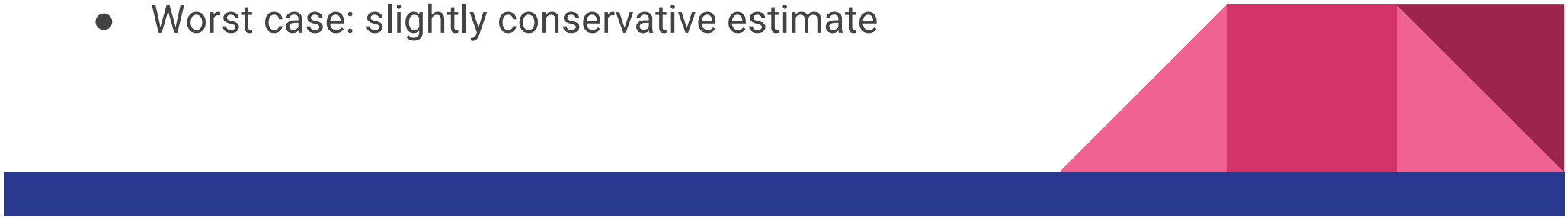
Backscatter conclusion

Assumptions Recap

1. Address Uniformity
2. Reliable Delivery
3. Backscatter Hypothesis

Conclusion

- Does good enough job
- Worst case: slightly conservative estimate

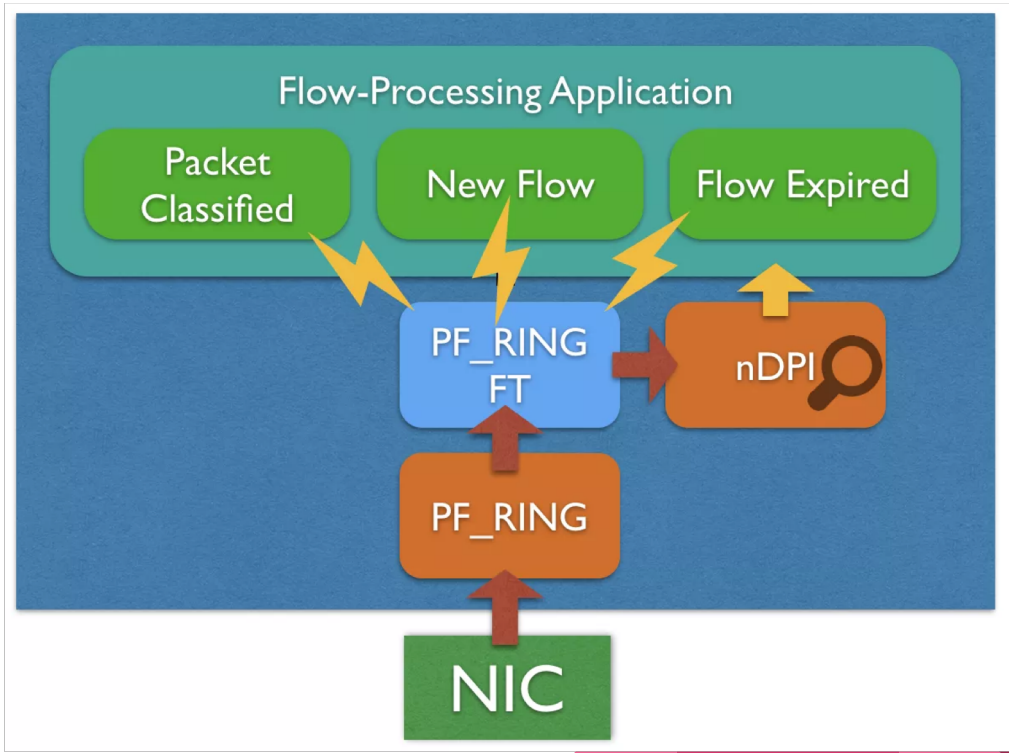


Analysis Methods

- Flow based Analysis
- Event Based Analysis

Flow Based Classification

- The definition of a flow
- Flow lifetime
- Minimum Requirements



Data Extracted from Flows

- TCP flag setting
- ICMP payload
- Address Uniformity
- Port Setting
- DNS Information
- Routing Information

Issues with Flow-based

- The flow parameters
- Highly variable attacks

Event-based Classification

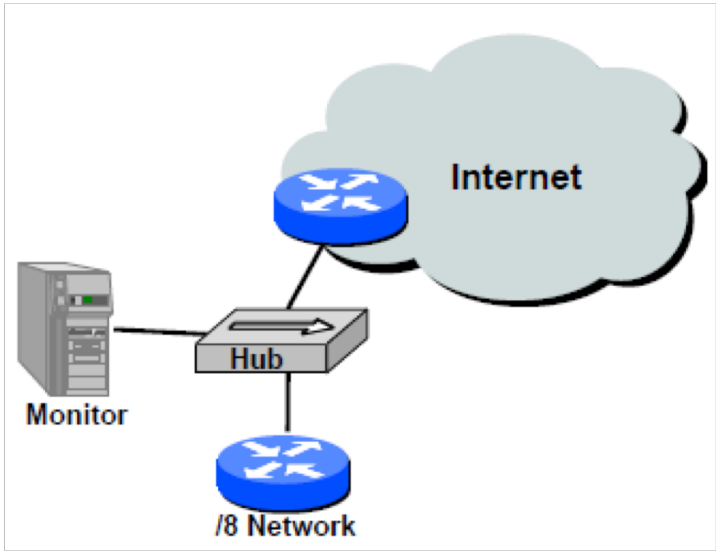
Focused entirely on the victim’s IP

Attack event definition

The goal of this approach

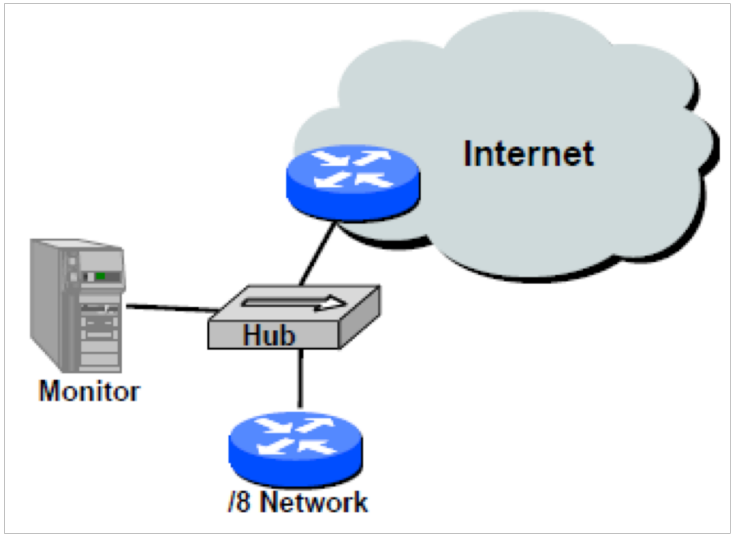
Experiment Setup

- 2^24 IP address (1/256 of the Internet address space)
- /8 network



Issues with the Setup

- Upstream router filtered some traffic
- Hijacked IP addresses



Data Gathered

12,805 attacks were observed over the week.

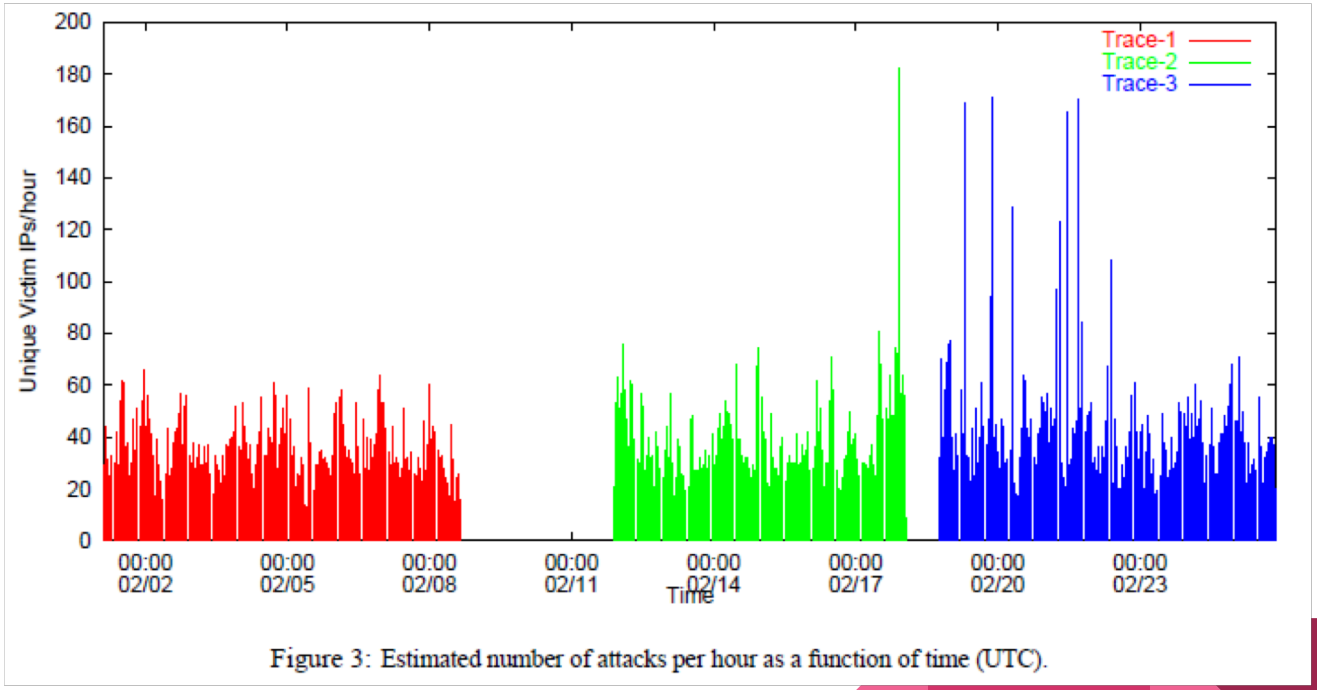


Figure 3: Estimated number of attacks per hour as a function of time (UTC).

Data Gathered cont'd

This table summarizes the data gathered using the flow and event based approaches

	Trace-1	Trace-2	Trace-3
Dates (2001)	Feb 01 – 08	Feb 11 – 18	Feb 18 – 25
Duration	7.5 days	6.2 days	7.1 days
Flow-based Attacks:			
Unique victim IPs	1,942	1,821	2,385
Unique victim DNS domains	750	693	876
Unique victim DNS TLDs	60	62	71
Unique victim network prefixes	1,132	1,085	1,281
Unique victim Autonomous Systems	585	575	677
Attacks	4,173	3,878	4,754
Total attack packets	50,827,217	78,234,768	62,233,762
Event-based Attacks:			
Unique victim IPs	3,147	3,034	3,849
Unique victim DNS domains	987	925	1,128
Unique victim DNS TLDs	73	71	81
Unique victim network prefixes	1,577	1,511	1,744
Unique victim Autonomous Systems	752	755	874
Attack Events	112,457	102,204	110,025
Total attack packets	51,119,549	78,655,631	62,394,290

Table 2: Summary of backscatter database.

Response Protocol

- 50% of the attacks and 20% of the back scatter packets are TCP with the RST flag set
- The next largest protocol category is ICMP host unreachable, comprising roughly 15% of the attacks

Kind	Trace-1		Trace-2		Trace-3	
	Attacks	Packets (k)	Attacks	Packets (k)	Attacks	Packets (k)
TCP (RST ACK)	2,027 (49)	12,656 (25)	1,837 (47)	15,265 (20)	2,118 (45)	11,244 (18)
ICMP (Host Unreachable)	699 (17)	2,892 (5.7)	560 (14)	27,776 (36)	776 (16)	19,719 (32)
ICMP (TTL Exceeded)	453 (11)	31,468 (62)	495 (13)	32,001 (41)	626 (13)	22,150 (36)
ICMP (Other)	486 (12)	580 (1.1)	441 (11)	640 (0.82)	520 (11)	472 (0.76)
TCP (SYN ACK)	378 (9.1)	919 (1.8)	276 (7.1)	1,580 (2.0)	346 (7.3)	937 (1.5)
TCP (RST)	128 (3.1)	2,309 (4.5)	269 (6.9)	974 (1.2)	367 (7.7)	7,712 (12)
TCP (Other)	2 (0.05)	3 (0.01)	0 (0.00)	0 (0.00)	1 (0.02)	0 (0.00)

Table 3: Breakdown of response protocols.

Attack Protocol

- 90% of the attacks use TCP as their protocol of choice
- Other Protocols represent a minor number of both attacks and back scatter

Kind	Trace-1		Trace-2		Trace-3	
	Attacks	Packets (k)	Attacks	Packets (k)	Attacks	Packets (k)
TCP	3,902 (94)	28,705 (56)	3,472 (90)	53,999 (69)	4,378 (92)	43,555 (70)
UDP	99 (2.4)	66 (0.13)	194 (5.0)	316 (0.40)	131 (2.8)	91 (0.15)
ICMP	88 (2.1)	22,020 (43)	102 (2.6)	23,875 (31)	107 (2.3)	18,487 (30)
Proto 0	65 (1.6)	25 (0.05)	108 (2.8)	43 (0.06)	104 (2.2)	49 (0.08)
Other	19 (0.46)	12 (0.02)	2 (0.05)	1 (0.00)	34 (0.72)	52 (0.08)

Table 4: Breakdown of protocols used in attacks.

Attack Protocol cont'd

Table 5 breaks down the data based off the service as revealed in the victims port number.

Kind	Trace-1		Trace-2		Trace-3	
	Attacks	Packets (k)	Attacks	Packets (k)	Attacks	Packets (k)
Multiple Ports	2,740 (66)	24,996 (49)	2,546 (66)	45,660 (58)	2,803 (59)	26,202 (42)
Uniformly Random	655 (16)	1,584 (3.1)	721 (19)	5,586 (7.1)	1,076 (23)	15,004 (24)
Other	267 (6.4)	994 (2.0)	204 (5.3)	1,080 (1.4)	266 (5.6)	410 (0.66)
Port Unknown	91 (2.2)	44 (0.09)	114 (2.9)	47 (0.06)	155 (3.3)	150 (0.24)
HTTP (80)	94 (2.3)	334 (0.66)	79 (2.0)	857 (1.1)	175 (3.7)	478 (0.77)
0	78 (1.9)	22,007 (43)	90 (2.3)	23,765 (30)	99 (2.1)	18,227 (29)
IRC (6667)	114 (2.7)	526 (1.0)	39 (1.0)	211 (0.27)	57 (1.2)	1,016 (1.6)
Authd (113)	34 (0.81)	49 (0.10)	52 (1.3)	161 (0.21)	53 (1.1)	533 (0.86)
Telnet (23)	67 (1.6)	252 (0.50)	18 (0.46)	467 (0.60)	27 (0.57)	160 (0.26)
DNS (53)	30 (0.72)	39 (0.08)	3 (0.08)	3 (0.00)	25 (0.53)	38 (0.06)
SSH (22)	3 (0.07)	2 (0.00)	12 (0.31)	397 (0.51)	18 (0.38)	15 (0.02)

Table 5: Breakdown of attacks by victim port number.

Attack Rate

- An attack rate of 500 SYN packets per second is enough to overwhelm a server
- Comparing the distributions, the uniform random attacks have a lower rate than the distribution of all attacks.
- A significant factor in the question of threat posed by an attack is the connectivity of the victim.

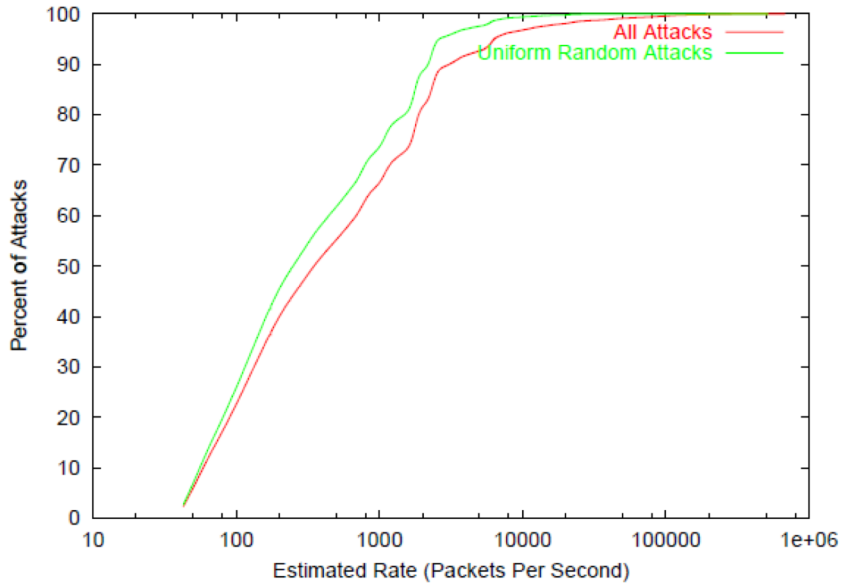


Figure 4: Cumulative distributions of estimated attack rates in packets per second.

Attack Duration

The following Graphs use Flow based classification due to the better characterization of attack durations while being immune to the intensity

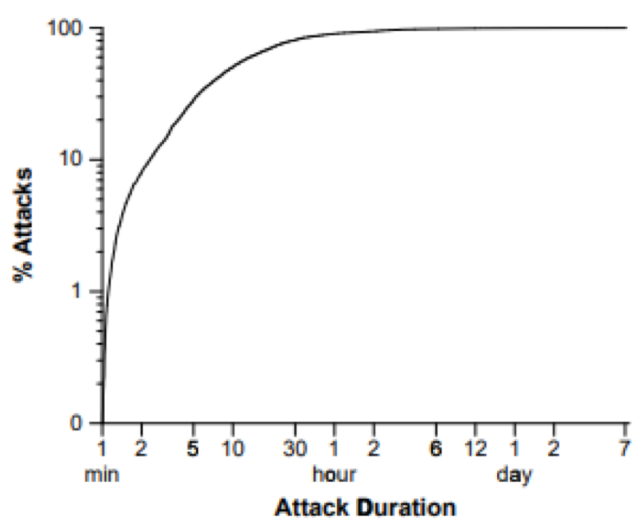


Figure 5: Cumulative distribution of attack durations.

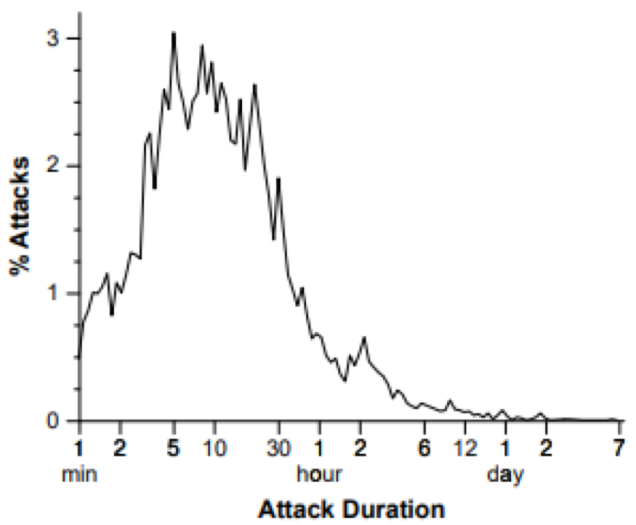


Figure 6: Probability density of attack durations.

Victim Classification

- DNS
- Top-level Domain
- Autonomous Systems
- Degree of Repeated Attacks

DNS

- A significant fraction of attacks directed at home machines
- “the.feds.cant.secure.their.shellz.ca”
- Internet Relay Chats, Multiplayer game sites, and Sexually suggestive sites tend to be victims as well

Kind	Trace-1				Trace-2				Trace-3			
	Attacks		Packets (k)		Attacks		Packets (k)		Attacks		Packets (k)	
Other	1,917	(46)	19,118	(38)	1,985	(51)	25,305	(32)	2,308	(49)	17,192	(28)
In-Addr Arpa	1,230	(29)	16,716	(33)	1,105	(28)	24,645	(32)	1,307	(27)	26,880	(43)
Broadband	394	(9.4)	9,869	(19)	275	(7.1)	13,054	(17)	375	(7.9)	8,513	(14)
Dial-Up	239	(5.7)	956	(1.9)	163	(4.2)	343	(0.44)	276	(5.8)	1,018	(1.6)
IRC Server	110	(2.6)	461	(0.91)	88	(2.3)	2,289	(2.9)	111	(2.3)	6,476	(10)
Nameserver	124	(3.0)	453	(0.89)	84	(2.2)	2,796	(3.6)	90	(1.9)	451	(0.72)
Router	58	(1.4)	2,698	(5.3)	76	(2.0)	4,055	(5.2)	125	(2.6)	682	(1.1)
Web Server	54	(1.3)	393	(0.77)	64	(1.7)	5,674	(7.3)	134	(2.8)	730	(1.2)
Mail Server	38	(0.91)	156	(0.31)	35	(0.90)	71	(0.09)	26	(0.55)	292	(0.47)
Firewall	9	(0.22)	7	(0.01)	3	(0.08)	3	(0.00)	2	(0.04)	1	(0.00)

Table 6: Breakdown of victim hostnames.

Top-level Domain

- TLDs are attacked the same percentage each week
- The com and net domains were each targeted 15% of the time
- Edu and org were the targets 3% of the time

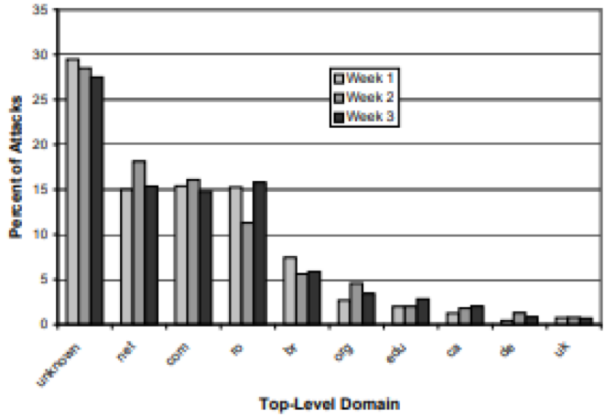


Figure 7: Distribution of attacks to the 10 top-level domains (TLDs) that received the most number of attacks.

Autonomous System

- No single AS or small set of ASes is the target of an overwhelming fraction of attacks.
- ASes experienced more variation in the number of attacks targeted at them for each week compared to TLDs.

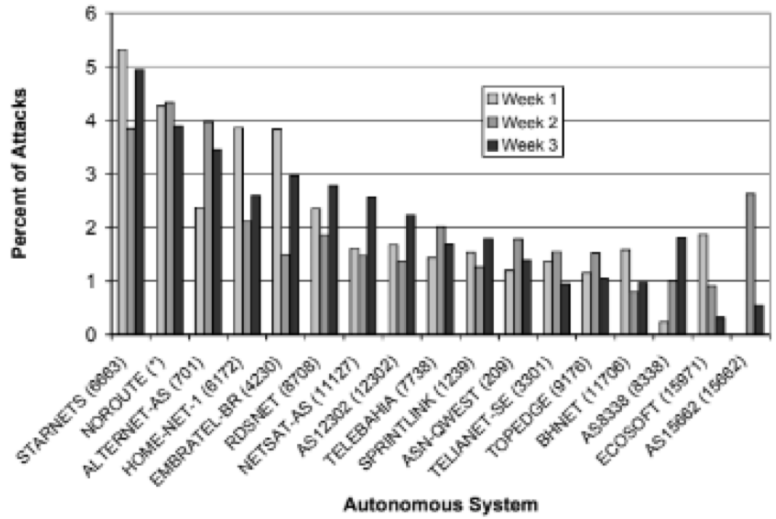


Figure 8: Distribution of attacks to Autonomous Systems (ASes) that were targeted by at least 1% of all attacks.

Victims of Repeated Attacks

- 65% of victims were attacked once
- 18% were attacked twice
- 12% were attacked less than 5 times

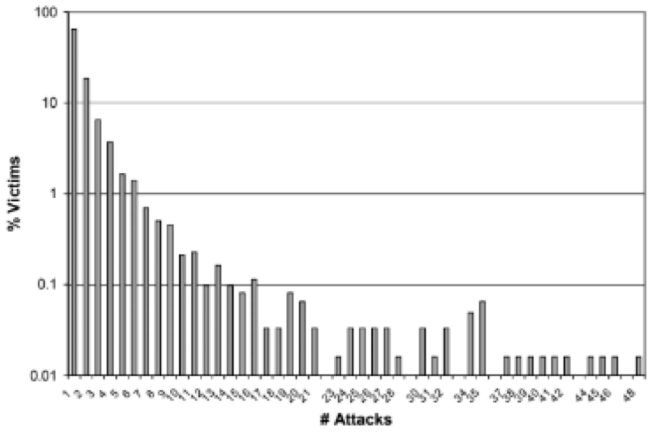


Figure 9: Histogram counting the number of victims of repeated attacks across all traces.

Validation

The Backscatter hypothesis states that unsolicited packets represent responses to spoofed attack traffic

Kind	Trace-1		Trace-2		Trace-3	
	Attacks	Packets (k)	Attacks	Packets (k)	Attacks	Packets (k)
TCP (RST ACK)	2,027 (49)	12,656 (25)	1,837 (47)	15,265 (20)	2,118 (45)	11,244 (18)
ICMP (Host Unreachable)	699 (17)	2,892 (5.7)	560 (14)	27,776 (36)	776 (16)	19,719 (32)
ICMP (TTL Exceeded)	453 (11)	31,468 (62)	495 (13)	32,001 (41)	626 (13)	22,150 (36)
ICMP (Other)	486 (12)	580 (1.1)	441 (11)	640 (0.82)	520 (11)	472 (0.76)
TCP (SYN ACK)	378 (9.1)	919 (1.8)	276 (7.1)	1,580 (2.0)	346 (7.3)	937 (1.5)
TCP (RST)	128 (3.1)	2,309 (4.5)	269 (6.9)	974 (1.2)	367 (7.7)	7,712 (12)
TCP (Other)	2 (0.05)	3 (0.01)	0 (0.00)	0 (0.00)	1 (0.02)	0 (0.00)

Table 3: Breakdown of response protocols.

Other Techniques

Sequential Change-Point Detection

- Statistics based approach
- Compares actual traffic with expected traffic

Activity Profiling

- Monitors average packet rate for network flow
- Groups flows by similar packet fields

Detection

- Can detect increase by single user (DoS)
- Can detect increase in number of users (DDoS)

Conclusion

- The only publically available data on DoS activity
- Better understanding of the nature of today’s threats
- Baseline for longer-term comparison and analysis

References

David Moore, Geoffrey M. Voelker, and Stefan Savage. Inferring Internet Denial-of-Service Activity. August 2000.

A.G. Tartokovsky, B.L. Rozovskii, R.B. Blazek, Hongjoong Kim. A novel approach to detection of intrusions in computer networks via adaptive sequential and batch-sequential change-point detection methods. In *IEEE Transactions on Signal Processing,* 54(9) September. 2006

Discussion Questions

1. Why would you want to measure the amount of Internet DoS attacks?
2. Is the assumption of uniform source addresses justifiable?
3. What other metrics can be found from the raw backscatter data?
4. Would this method, capturing backscatter, still work today for detecting DoS attacks?