DDoS Research

Yue Duan
Illinois Institute of Technology

Inferring Internet Denial-of-Service Activity

David Moore, Geoffrey M. Voelker and Stefan Savage;

University of California, San Diego

Usenix Security 2001

Outline

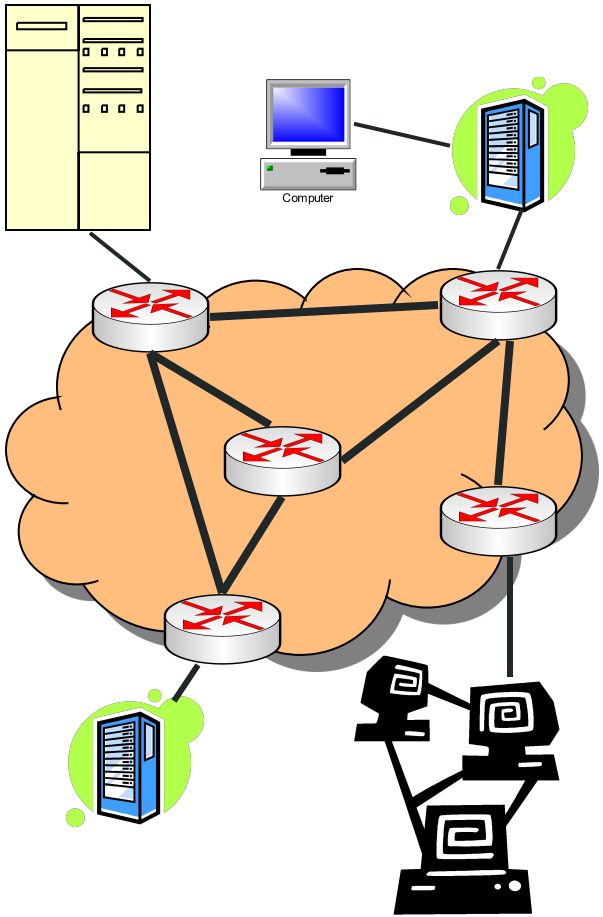
- Contribution
- Motivation
- Introduction of Denial-of-Service (DoS) Attacks
- Basic Methodology
- Attack Classification
- Results

Contribution

- Presented a novel technique “backscatter analysis” to estimate the worldwide DoS activity
- Performed three-week long real experiments and classified the DoS attacks quantitatively

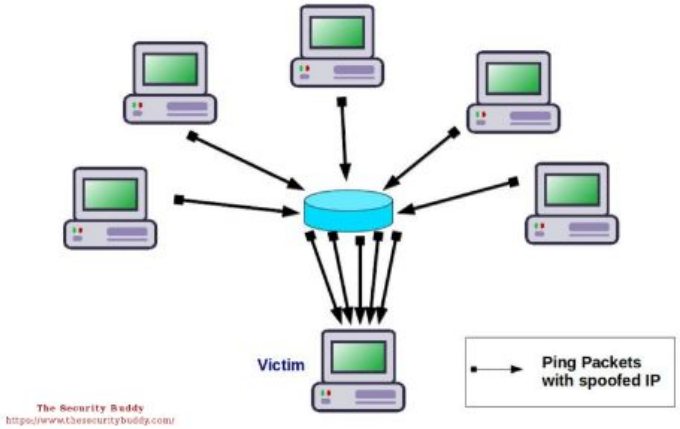
Motivation

- How prevalent are DoS attacks in the Internet today?
  - How often?
  - What attack protocols used?
  - Attack rate?
  - Attack duration?
  - Victim names and domains?
  - And more ...



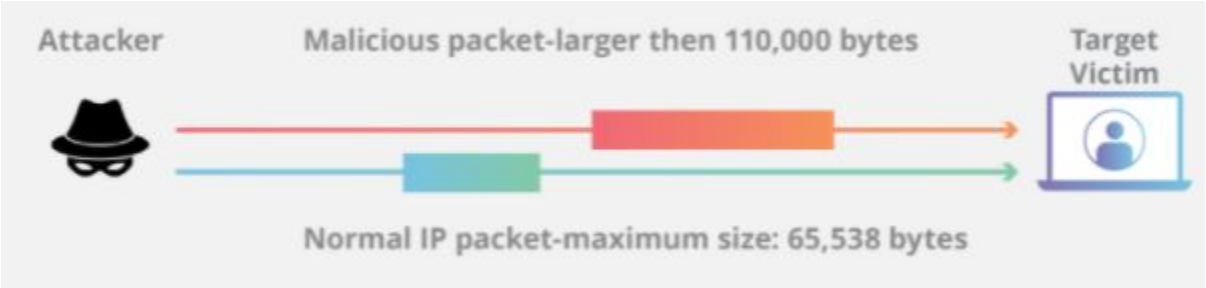
DoS Attack Introduction

- Consume resources of a host or network
- Logic attacks: software flaws
  - Ping-of-Death
- Flooding attacks: overwhelm CPU, memory or network resources
  - SYN flood
  - TCP ACK, NUL, RST and DATA floods
  - ICMP Echo Request floods
  - And so on ...



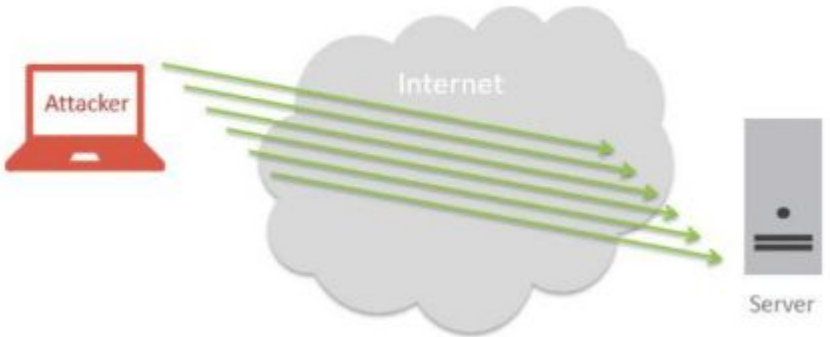
DoS Attack Introduction

- Ping-of-Death
  - IP4 ping packets can be as large as 65,535 bytes
  - What if there is a malicious packet exceed the limit?
  - The total size exceeds the size limit and a buffer overflow can occur, causing the target machine to freeze, crash or reboot.



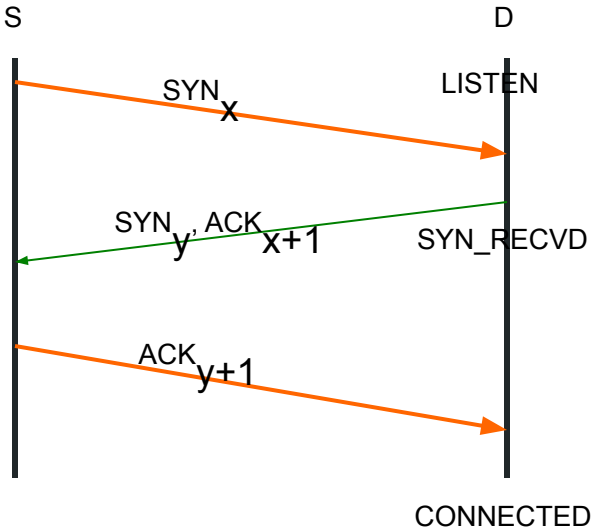
DoS Attack Introduction

- DoS: Flood attacks
  - 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

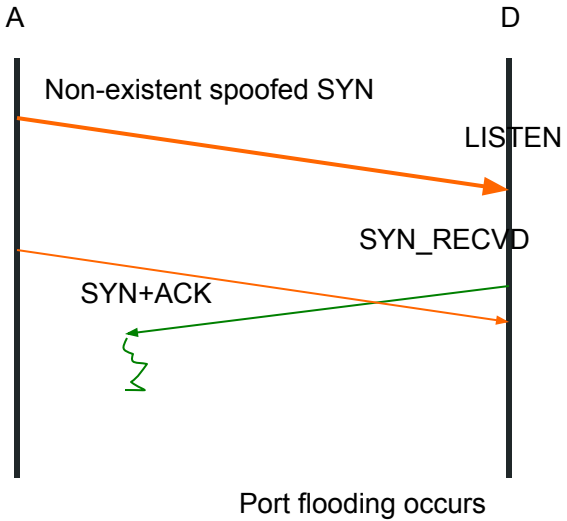


DoS Attack Introduction

- SYN flood

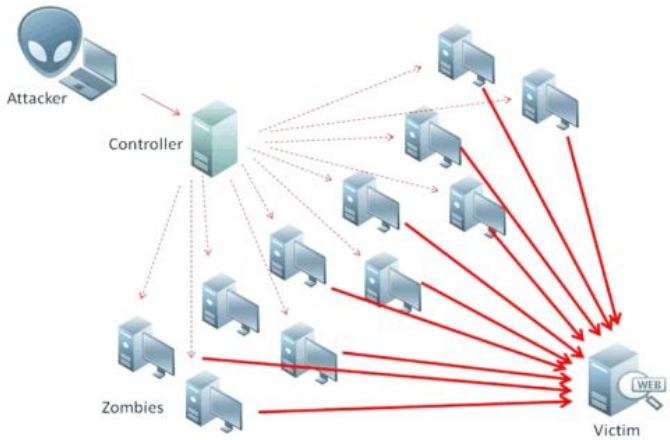


- TCP RST



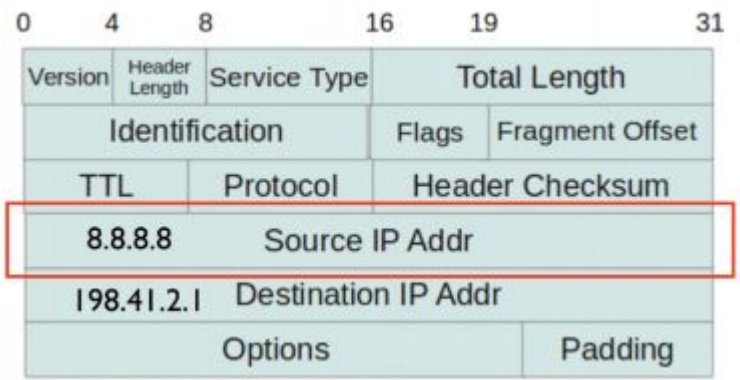
DoS Attack Introduction

- Distributed denial-of-service attack (DDoS)
  - Control a group of “zombie” hosts to launch assault on specific target(s)
  - A botnet can perform the DDoS attacks



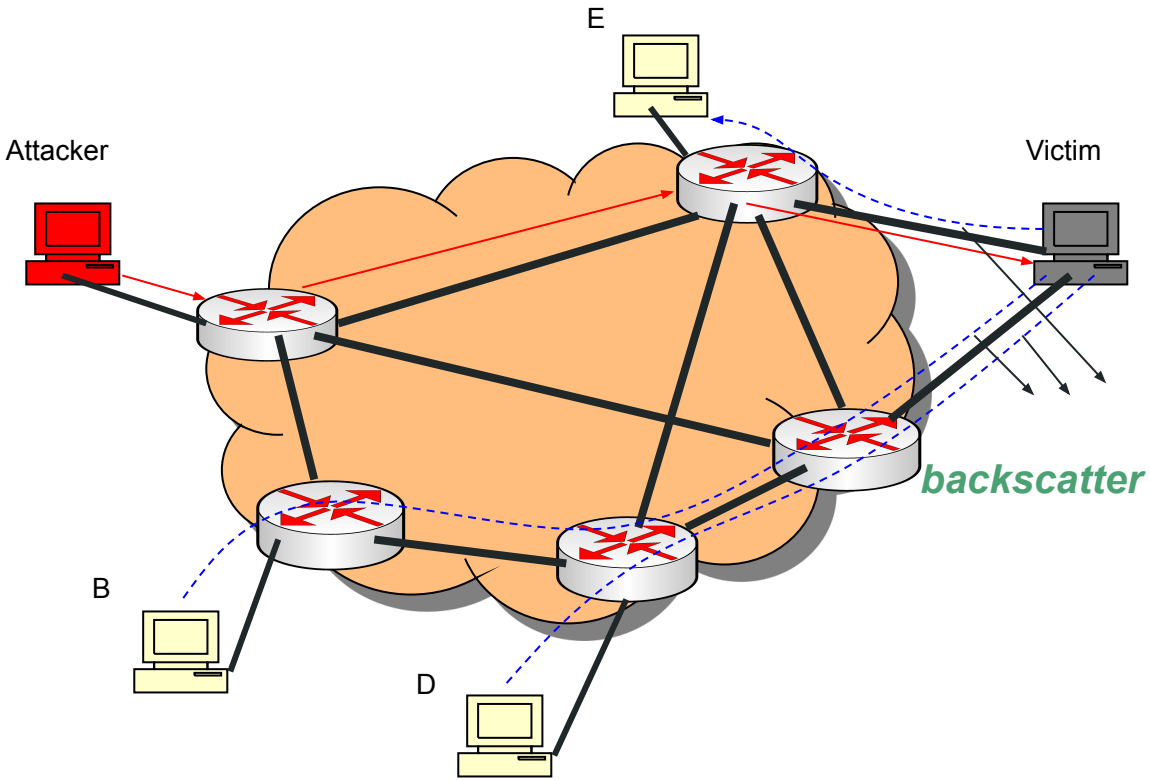
DoS Attack Introduction

- IP spoofing
  - Attackers forge IP source addresses
  - Simple technique but very difficult to trace-back



Basic Methodology - Backscatter

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



Basic Methodology - Backscatter

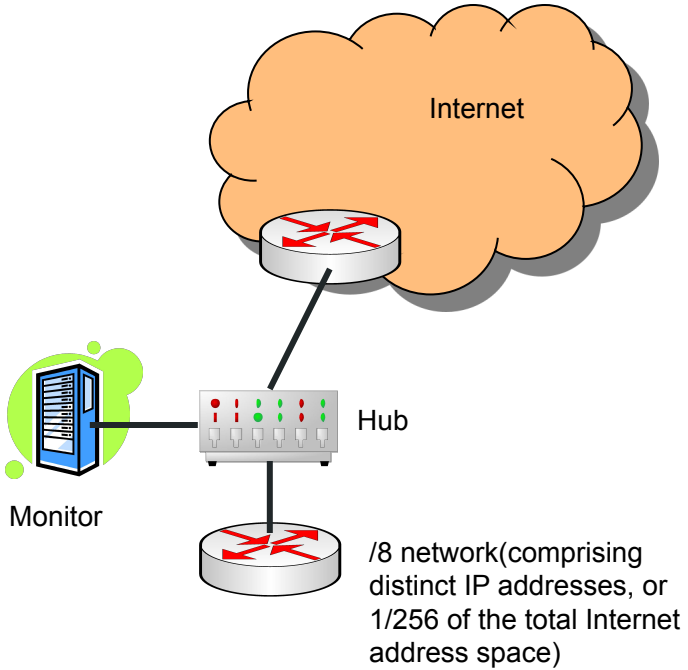
- Main assumptions:
  - Address uniformity
  - Reliable delivery
  - Backscatter hypothesis
- Secondary assumptions:
  - One response, by victim, for every packet in attack
  - Monitors can capture backscatter

Basic Methodology - Backscatter

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

$$E(x) = \frac{nm}{2^{32}} = \frac{m}{256}$$

n - # distinct IP addresses monitored
m - # attacking packets



Basic Methodology - Backscatter

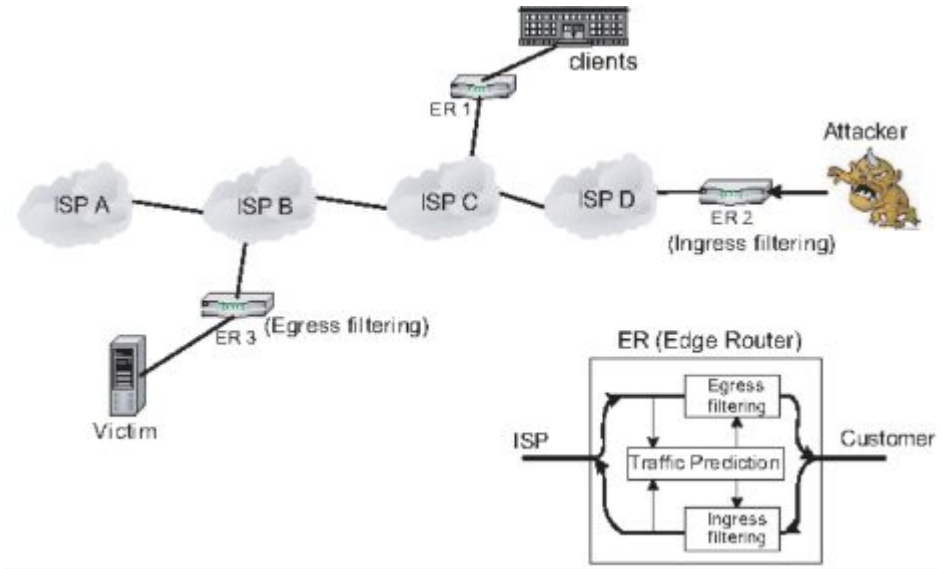
- Metrics
  - Victim identity
  - Type of attack
  - Timestamp
  - Average arrival rate

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.

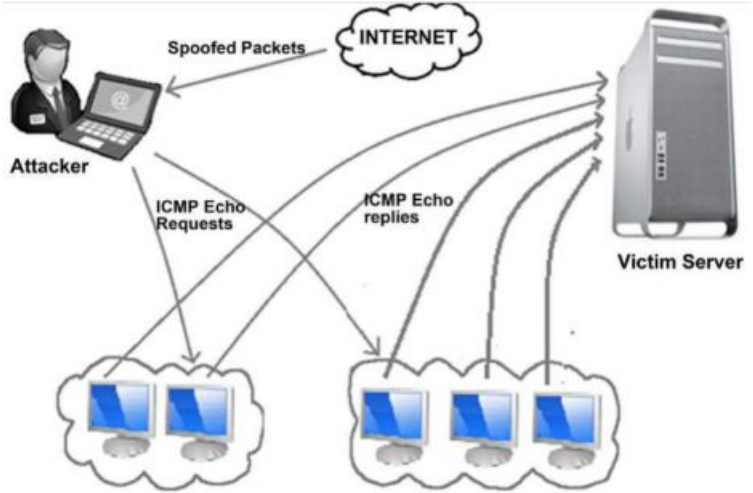
Backscatter Accuracy/Biases

- Ingress filtering
  - Deployed by ISP
  - Filters out spoofed packets
- Effect On Backscatter
  - Packets could be dropped
  - Harder to detect DoS attempt



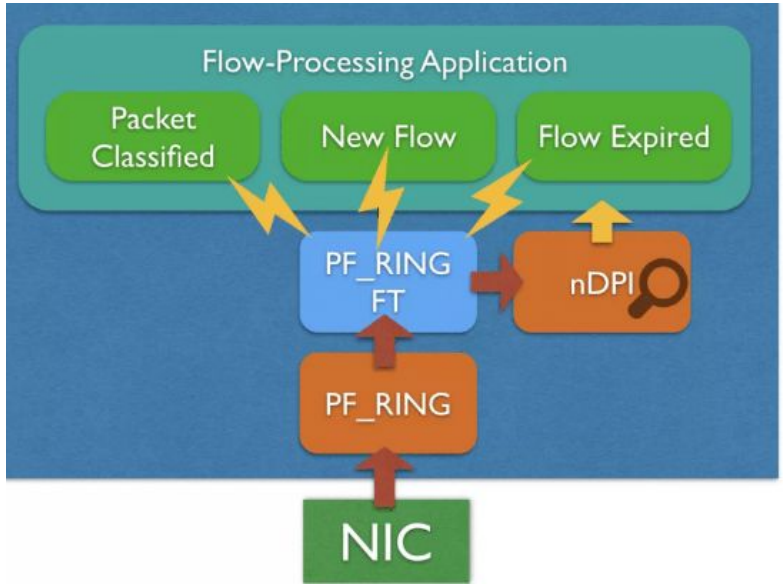
Backscatter Accuracy/Biases

- 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



Attack Classification

- Flow-based classification
  - A flow is a series of consecutive packets sharing the same target IP address and IP protocol
  - Flow lifetime: fixed five-minute approach
  - Reduce noise and misconfiguration traffic by setting thresholds
  - Extract packet information from flows

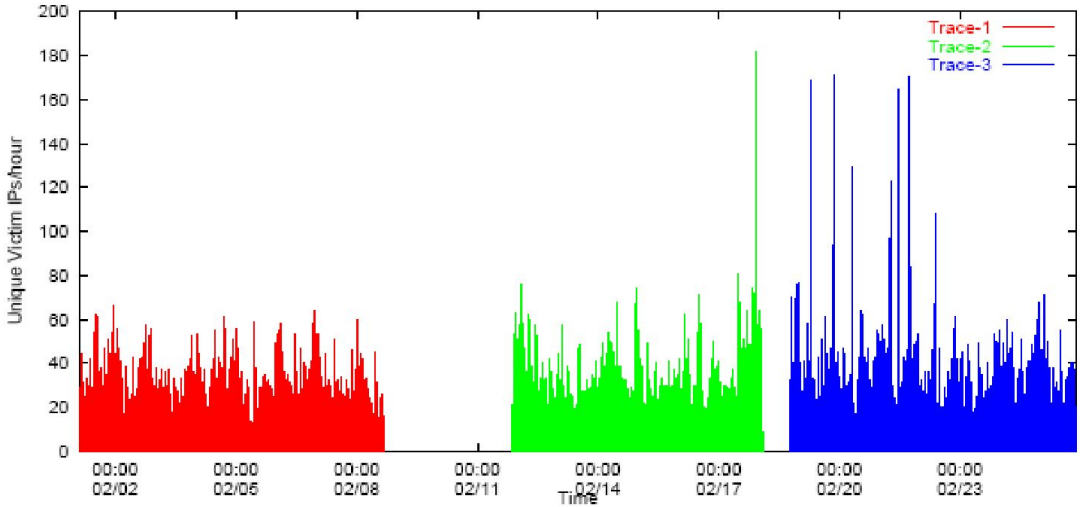


Attack Classification

- Event-based classification
  - Flow-based obscures time-domain characteristics
  - Focused entirely on the victim’s IP
  - An attack event is defined by a victim emitting at least ten backscatter packets in one minute

Experiment

- 12,805 attacks were observed over a week



Estimated number of attacks per hour as a function of time (UTC)

Experiment

	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

Experiment

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

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)

Experiment

- 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

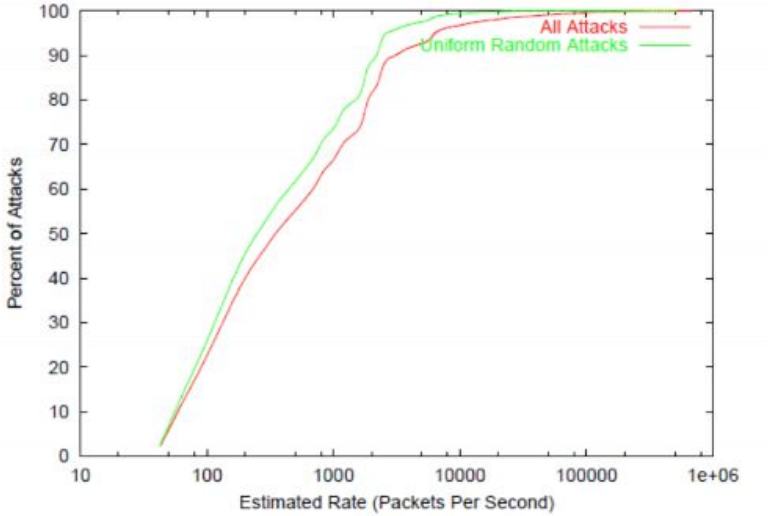


Figure 4: Cumulative distributions of estimated attack rates in packets per second.

Experiment

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

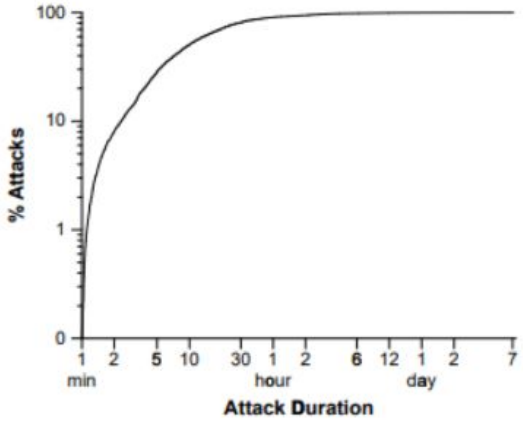


Figure 5: Cumulative distribution of attack durations.

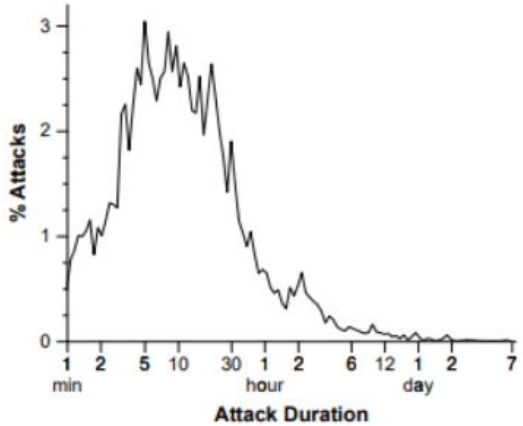


Figure 6: Probability density of attack durations.