Defending against Distributed Denial of Service Attacks: A Tutorial

Distributed Denial of Service Attacks

Outline

Denial of Service

DDoS Attacks

Solutions to DDoS Attacks

Performance of various queuing algorithms under DDoS Attack

Denial of Service Attacks

Denial-of-Service (DoS) attack is an attempt by attacker to prevent legitimate users from using resources

Denial-of-Service denies a victim (host, router, or entire network) from providing or receiving normal services

Denial of Service Attacks

- **Exploit system design weaknesses**
  - **Ping of death**
  - **Teardrop**

System patches issued after discovering such attacks

- **Computationally intensive tasks**
  - **Encryption and decryption computation**

Security mechanisms included in the protocols

- **DDoS attack (Flooding-Based)**
  - **Exploit the computing power of thousands of vulnerable, unpatched machines to overwhelm a target or a victim**
  - **CPU, Memory, bandwidth exhaustion**

The question to be answered!

Distributed Denial of Service (DDoS) Attacks

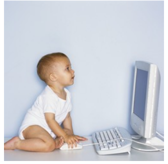
Do not depend on system or protocol weaknesses

Introduce the “many to one” dimension

Large number of compromised host are gathered to send useless service requests, packets at the same time

The burst of traffic generated, crashes the victim or disables it

Distributed Denial of Service (DDoS) Attacks (Elements)



Victim (Target)

- receives the brunt of the attack

Attack Daemon Agents

- agent programs that actually carry out the attack on victim
- attacker gain access and infiltrate the host computer to deploy them
- daemons affect both the target and the host computers

Master Program/Agent

- coordinates the attack through the attack daemons

Attacker/Attacking Hosts

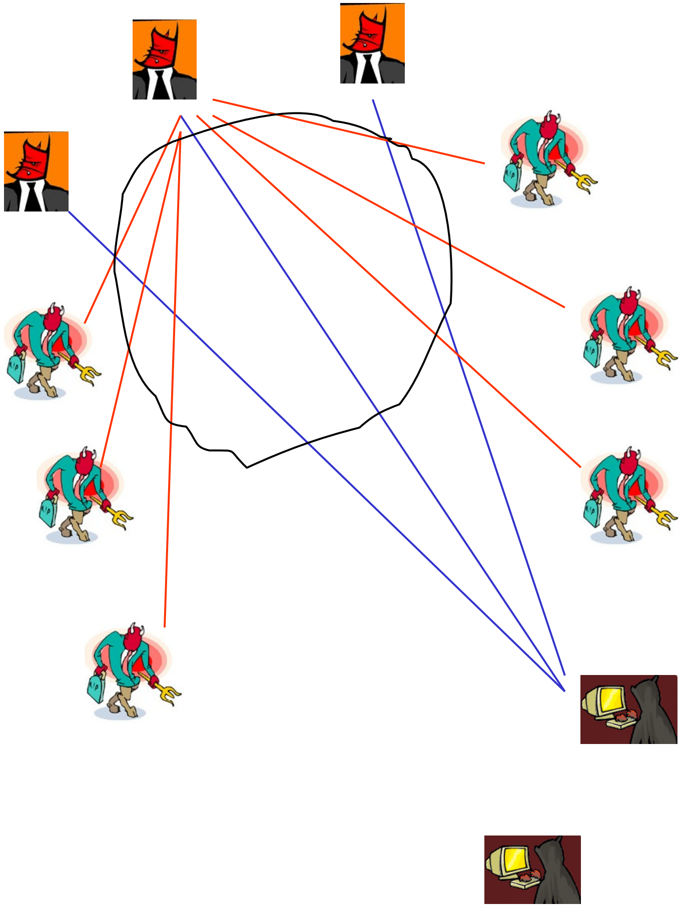
- mastermind behind the attack

Typical Distributed Denial of Service (DDoS) Attacks

In preparation for launching an attack, attacker sets up a DDoS attack network

- **one or more attacking hosts**
- **number of masters**
- **large number of attack daemons (also referred to as *`zombies`*)**

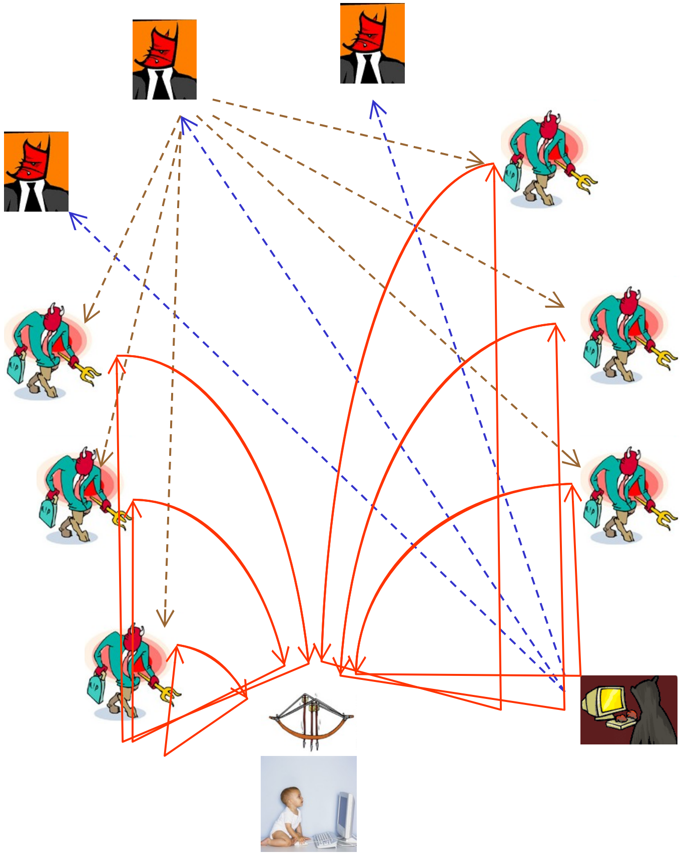
Each attacking host controls one or more masters



Typical Distributed Denial of Service (DDoS) Attacks (contd..)

With attack network ready

- Attack hosts launch an ‘attack’ command with
  - victim’s address
  - attack duration
  - attack method, etc
- Master program propagates the command to the attack daemons under its control



DDoS Attack Methods

- **SMURF**
  - **attacker sends large amount of ICMP echo traffic to a set of IP broadcast addresses with victim's spoofed address**
  - **most hosts accept these ICMP echo requests and respond to them with an echo reply to the source address, i.e. the targeted victim**
  - **multiplies traffic to the victim by number of responding hosts**

  - **On a broadcast network, potentially hundreds of hosts could reply to each ICMP Packet**
  - **This process of using intermediate network devices to elicit many responses to a single packet has been labeled as an "amplifier" process**
  - **amplifier as well as the target victim are impacted**
  - **This method overloads an entire network**

DDoS Attack Methods (contd…)

- **SYN Flood (TCP SYN Attack)**
  - **Exploits TCP 3-way handshake**
  - **attacker sends barrage of initial SYNs with spoofed addresses leaving the victim in half-open state, waiting for the non-existent ACKs and retransmitting**
  - **victim's resources for new connections exhausted by these half-open connections**

- **UDP Flood**
  - **based on UDP echo and character generator services**
  - **attacker uses forged UDP packets to connect the echo service on one machine to the character generator (chargen) service on another machine**
  - **resultant- the two services consume all available network bandwidth**

Question-

Why use the particular combination of echo & chargen?

DDoS Tools and Their Attack Methods

Trinoo	**UDP**
Tribe Flood Network (TFN)	**UDP, ICMP, SYN, Smurf**
Stacheldracht	**UDP, ICMP, SYN, Smurf**
TFN 2K	**UDP, ICMP, SYN, Smurf**
Shaft	**UDP, ICMP, SYN**

www.csl.mtu.edu/cs6461/www/Slide/ddos5090.ppt

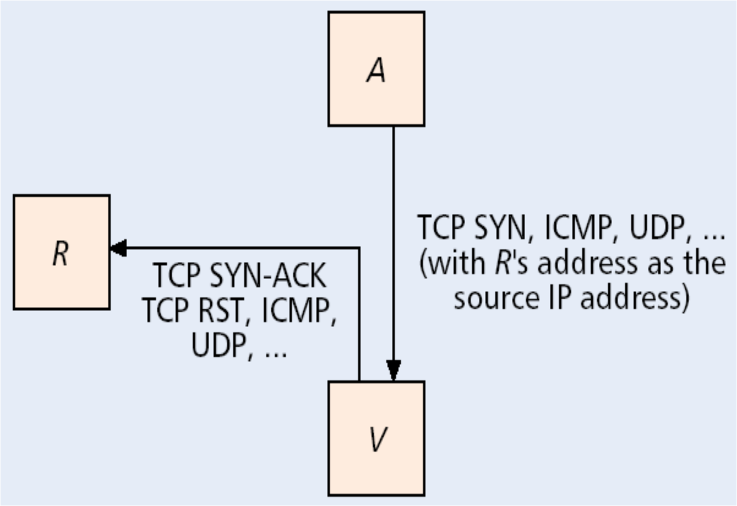
Direct Attacks

Attacker sends large number of packets directly towards victim

- could use SMURF, TCP SYN Flood, UDP Flooding, or a mixture
- another variant of TCP based attack causes the victim to respond with RST packets

As per one measurement, attack methods in Internet

- TCP packets based attacks – 94%
- UDP packets based attacks – 2%
- ICMP packets based attacks – 2%



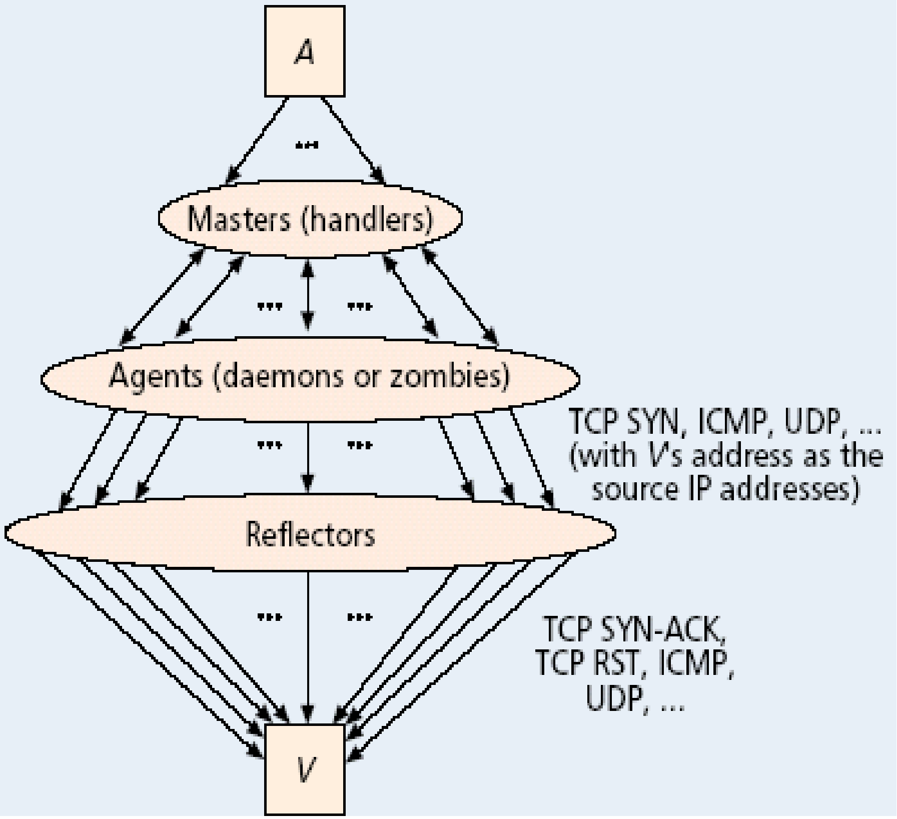
Reflector Attacks

indirect attack

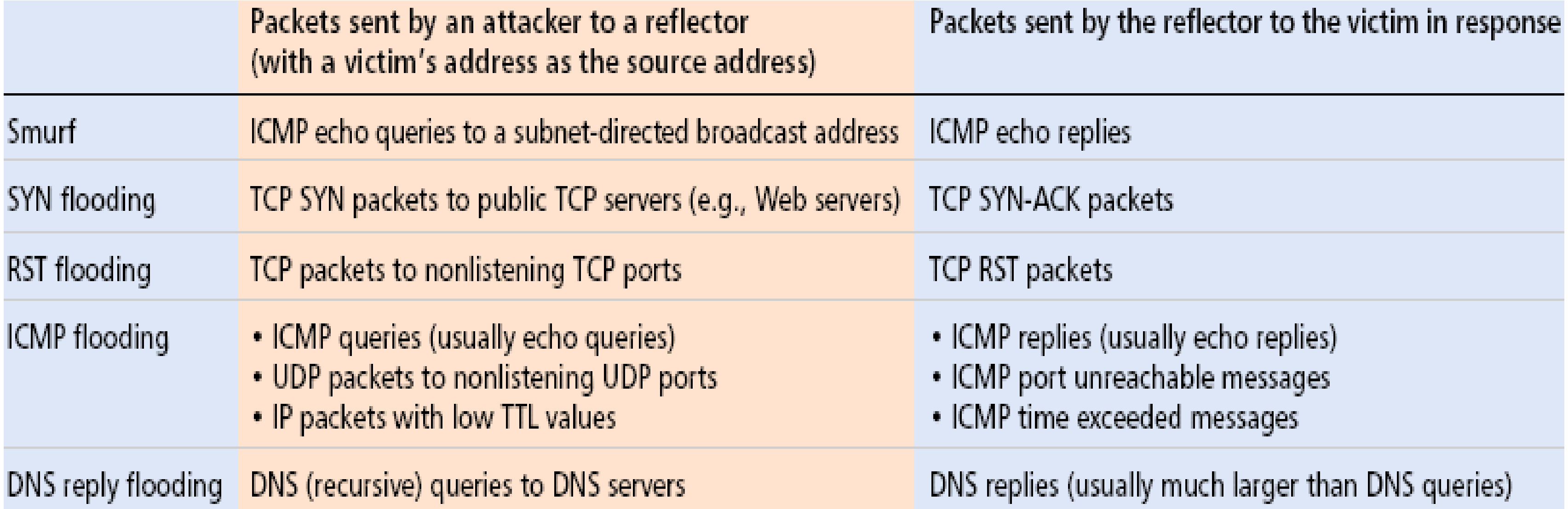
uses intermediary nodes (routers & servers), to act as *innocent* attack launchers – return response packets to the victim in reply to spoofed packets sent by attack daemons

attack packets reflected in the form of normal packets by intermediary nodes, thus they act as 'reflectors/amplifiers'

capitalizes on a protocol's ability to automatically generate response messages



Reflector Attack (examples)



	Packets sent by an attacker to a reflector (with a victim's address as the source address)	Packets sent by the reflector to the victim in response
Smurf	ICMP echo queries to a subnet-directed broadcast address	ICMP echo replies
SYN flooding	TCP SYN packets to public TCP servers (e.g., Web servers)	TCP SYN-ACK packets
RST flooding	TCP packets to nonlistening TCP ports	TCP RST packets
ICMP flooding	• ICMP queries (usually echo queries) • UDP packets to nonlistening UDP ports • IP packets with low TTL values	• ICMP replies (usually echo replies) • ICMP port unreachable messages • ICMP time exceeded messages
DNS reply flooding	DNS (recursive) queries to DNS servers	DNS replies (usually much larger than DNS queries)

Minimal Rate of attack packets arrival at victim

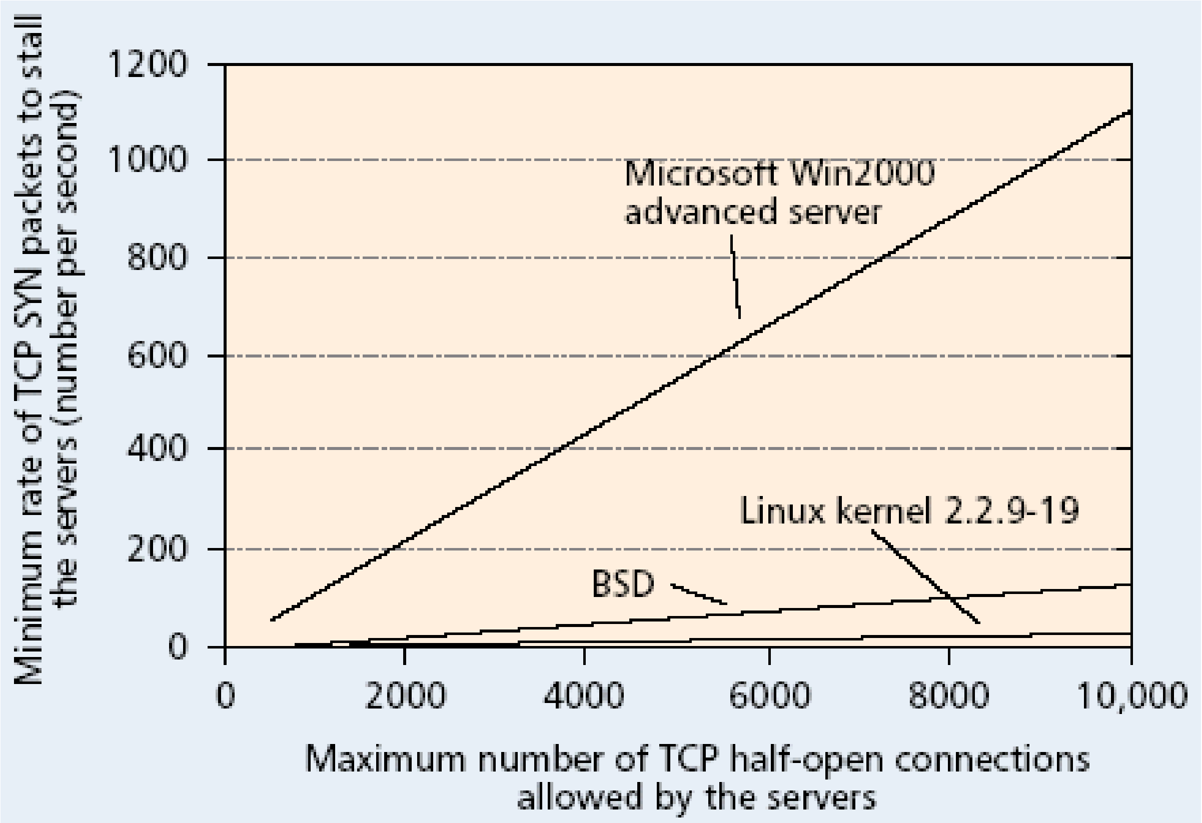
SYN Flooding

- Maximum Lifetime of Half-open connections
  - MS Windows2K Advanced Server – 9 sec
  - BSD – 75 sec
  - Linux Kernel 2.2.9-19 – 309 sec
- for 84 byte long SYN datagram
  - 56 kbps connection sufficient to stall Linux & BSD servers with number of half-open connections, N <= 6000
  - 1 Mbps rate sufficient to stall all of above three servers with N <= 10,000

ICMP Ping Flooding

- aggregated attack traffic of atleast 1.544 Mbps to jam a T1 link
- at 1 pkt/sec, around 5000 agents/reflectors needed to flood victim’s T1 link

Minimal Rate of attack packets arrival at victim (contd…)



Classification of solutions

- **Attack prevention and preemption (before the attack)**
- **Attack detection and filtering (during the attack)**
- **Attack source traceback and identification (during and after the attack)**

Attack prevention and Preemption

- **Passive side**
  - **Detect master and agent implants by signatures and scanning procedures on the hosts**
  - **Monitor network traffic for known attack messages sent between attackers and masters**
- **Active side**
  - **Intercept attack plans by employing cyber-informants and cyber-spies**

Attack prevention and Preemption
(contd..)

Unfortunately,

- **Many careless users (or they do not know how to ‘care’)**
- **ISP and enterprise networks are not willing to monitor for attack**
- **Attack plans require in-depth knowledge of attack method while it could be changed by attackers realtime-ly to avoid detection**

Attack Source Traceback and Identification

Locate the criminal after the attack –identify the source of any packet without looking at its may-be-spoofed header

- **Record bypassing packets info at routers**
- **Give every packet’s destination additional information (not sure how this works)**

Attack Source Traceback and Identification
(contd..)

Infeasibility of these methods

- **Current IP traceback solutions sometimes doesn’t work (attackers behind firewall or NATs)**
- **Might involve legitimate sources who innocently act as the reflectors**
- **Even if malicious sources are detected, stopping them is very difficult (esp. when they are distributed across various ASs)**

Conclusion

- **IP traceback - not so effective, but still indispensable**

Attack Detection and Filtering

Detection

Filtering

Detection is easy, filtering is hard

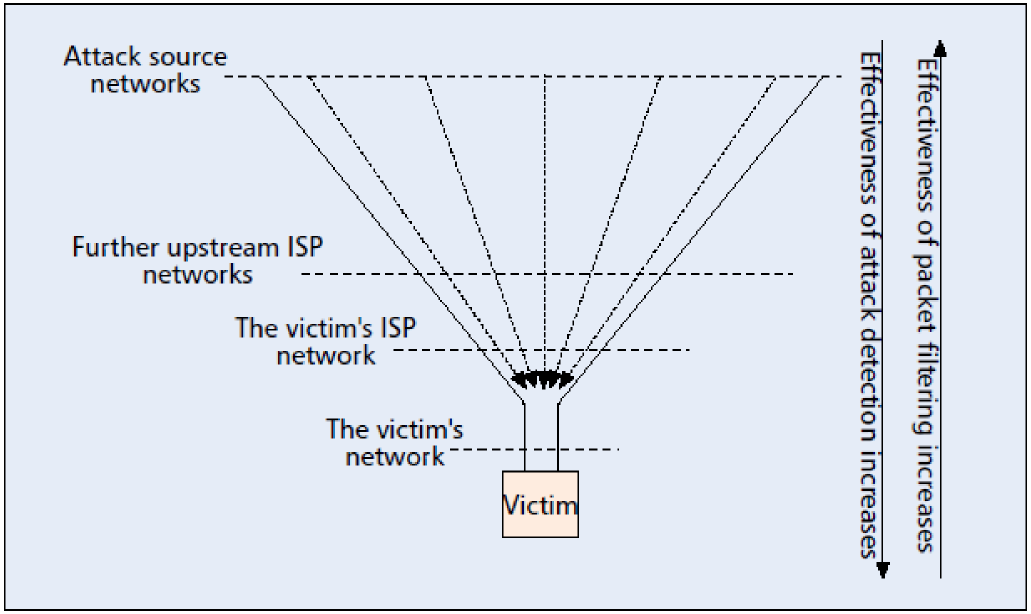
Filtering Metrics

- **False positive ratio (FPR), false negative ratio (FNR) – the effectiveness of telling good from bad**
- **Normal packet survival ratio (NPSR) – a reverse metric to FPR, could be just 1-FPR**

Attack Detection and Filtering

(contd..)

During typical large-scale DDoS attacks, a victim is usually doomed (or sacrificed). Nothing can be sent or received by it.


Attack source networks
Further upstream ISP networks
The victim's ISP network
The victim's network
Victim
Effectiveness of attack detection increases
Effectiveness of packet filtering increases

■ Figure 4. *Possible locations for performing DDoS attack detection and filtering.*

Attack Detection and Filtering

At Source Networks

- Gladly,

  Spoofed packets can easily be detected and dropped

  If an attack packet is not spoofed (i.e, in direct attack), the source, namely the agent, can be traced

- Sadly,

  If spoofed packets contain valid IP address then they can not be detected (i.e, in the same subnet)

  Asking all ISP networks to install ingress packet filtering is also a Mission Impossible

Attack Detection and Filtering

At the victim’s Network

- Detection is easy, normally based on traffic anomaly (see [11] for more details)

Approaches other than detect-and-filter

- IP hopping (moving target defense) – victim changes its IP when being attacked. However, the victim still can be found by DNS tracing
- Proxying TCP connection requests (to deal with SYN flooding)

  Son : Daddy, help!

  Dad: No problem my boy! See how I will kick his ass!

  (After several mins) The Dad went unconscious and the crying boy ran to find his grandpa

Attack Detection and Filtering

At a Victim’s Upstream ISP Network

- Usually, we do nothing
- After detecting an attack, the victim network may notify the upstream ISP router the feature of the attack flows based on which the upstream ISP router filters packets
- The notification should be carefully designed
- Can’t be TCP
- Should be protected by strong authentication and encryption to avoid providing another hole for attacking

Attack Detection and Filtering

At Victim’s Upstream ISP Network (contd..)

- **The filter is not effective which eventually shuts down the victim’s network**

- **What if even grandpa is not strong enough?**

  Son (sobbing, finally found his grandpa): Grandpa, help!

  Grandpa: No problem my boy! See how I will kick his ass and avenge for your father!

  (After several mins) The Grandpa went unconscious and the crying boy ran to find his grandpa’s father (if he is still alive)

Internet Firewall

A global defense infrastructure attempts to detect attacks in the Internet core and drops the attack packets

Two proposals

- A route-based packet filtering (RPF)
- A Distributed Attack Detection approach (DAD – not that boy's Dad!)

Internet Firewall

A Route-Based packet filtering

- Extends the ingress packet filtering to the Internet core, filtering packet according to the inscribed source and destination addresses along with the BGP routing information

- Simulation shows its effectiveness (how to simulate it?)

- Drawbacks
  - Falsely drop legitimate packets due to recent route change
  - Add to the BGP message size and processing time
  - Too many filters need to be placed
  - Cannot filter packets with valid source addresses

Internet Firewall

A Distributed Attack Detection Approach

- A set of distributed detection systems (DSs) is employed to detection anomalies
- DSs cooperatively detect DDoS attacks by exchanging attack information derived from local observations
- Sophisticated mechanisms are needed to detect anomalies
- A separate channel is needed for them to communication

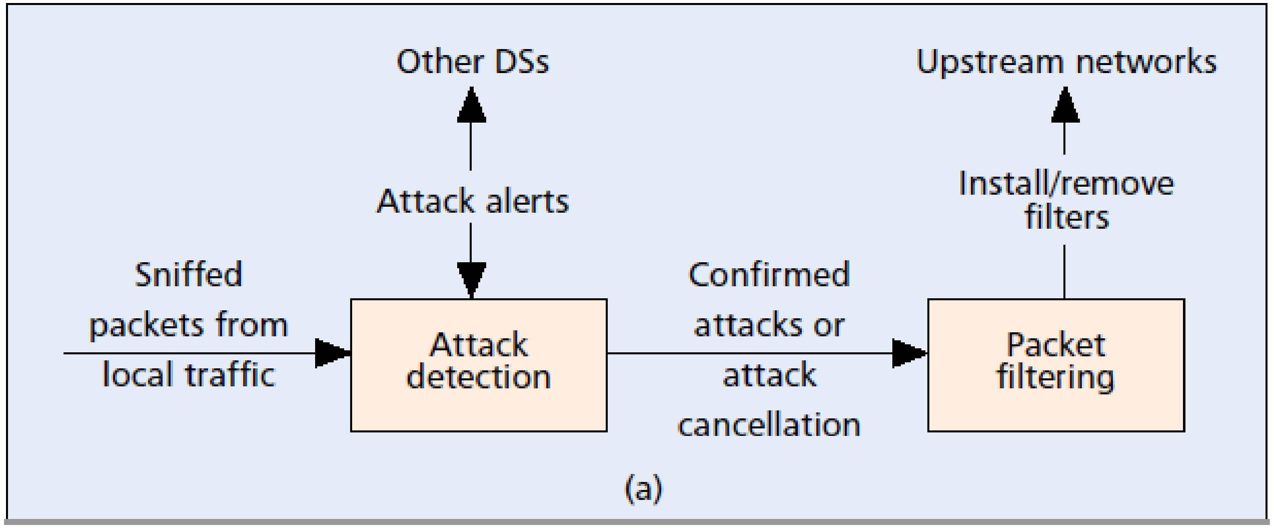
Internet Firewall

A Distributed Attack Detection Approach

- DAD is more practical as it requires much less ‘implant’
- Design of DAD
  - How to put them in the network to reduce the overhead to the least while maintaining effectiveness
  - How to coordinate them

Internet Firewall

A Distributed Attack Detection Approach

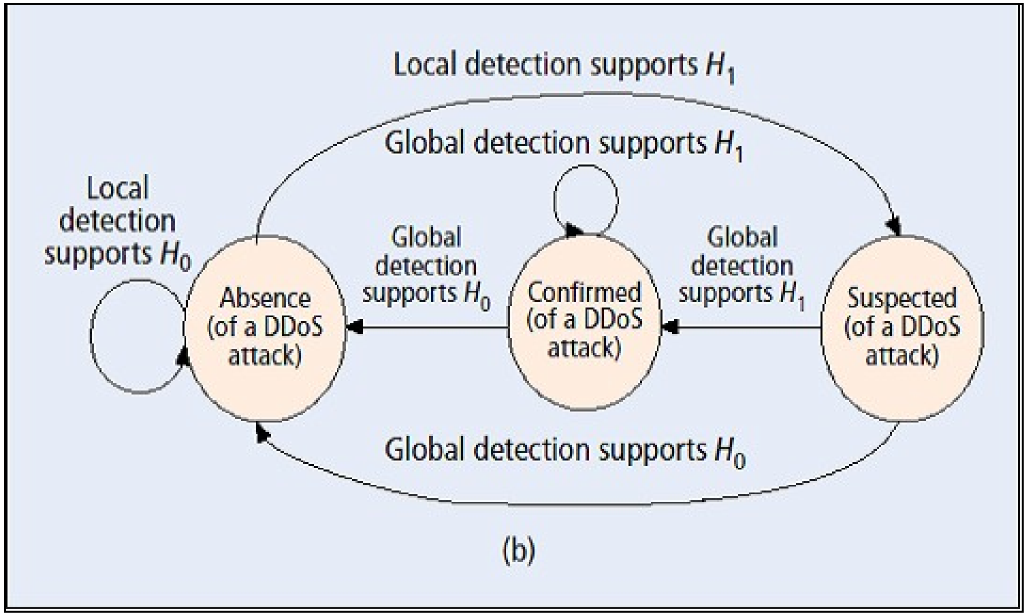


Internet Firewall

A Distributed Attack Detection Approach

H_1: Presence of a DDoS

H_0: Nothing unusual


Local detection supports H_1
Global detection supports H_1
Local detection supports H_0
Global detection supports H_0
Global detection supports H_1
Absence (of a DDoS attack)
Confirmed (of a DDoS attack)
Suspected (of a DDoS attack)
Global detection supports H_0

(b)

Internet Firewall

A Distributed Attack Detection Approach

- **Packet Filtering**
    - **Install filters on all switch interfaces at the beginning**
    - **DS identifies the involved interfaces**
    - **Remove filters on uninvolved interfaces**
- **To guarantee the connection between DSs**
    - **Intrusion Detection Exchange Protocol**
    - **Intrusion Detection Message Exchange Format**

Internet Firewall

A Distributed Attack Detection Approach

- **How to detect an attack as soon as possible**

For one DS moves from H_0 to H_1

- **Bayesian formulation**
- **Threshold-based decision rule**

Threshold-based method is used for global decision

	Ubiquitous ingress packet filtering (UIPF)	Route-based packet filtering (RPF)	Local attack detection (LAD)	Distributed attack detection (DAD)
1. Detection locations	All ISP networks that are connected to leaf networks in the Internet	A set of packet filters distributed in the Internet	Potential victims' networks and/or their upstream ISP networks	A set of detection systems distributed in the Internet
2. Filtering locations	Same as the detection locations	Same as the detection locations	Same as the detection locations and further upstream ISP networks if backpressure is used	Same as the detection locations and other upstream networks
3. Attack signatures	Spoofed source IP addresses	Spoofed source IP addresses according to the BGP routing information	Traffic anomalies and misuses detected by local intrusion detection systems	Mainly traffic anomalies observed from the set of distributed detection systems
4. False positive ratio (FPR)	= 0	= 0 if the BGP routes are correct	≥ 0 (= 1 in a sufficiently large-scale DDoS attack)	≥ 0 (high if the detection algorithms are overly sensitive)
5. False negative ratio (FNR)	≥ 0 (= 0 if all attack packets use spoofed addresses)	≥ 0 (small if most attack packets use spoofed addresses)	≥ 0 (= 0 in a sufficiently large-scale DDoS attack)	≥ 0 (high if the detection algorithms are not sensitive enough)
6. Normal packet survival ratio (NPSR)	≥ 0 (= 1 if all attack packets use spoofed addresses)	≥ 0 (large if most attack packets use spoofed addresses and the number of the AS nodes involved in the packet filtering is sufficiently large)	≥ 0 (= 0 in a sufficiently large-scale DDoS attack)	≥ 0 (high if both the false negative and positive ratios are low, and the set of detection systems are placed optimally in the Internet)
7. New communication protocols	Not required	Modifications to BGP protocols	Attack alert protocols between victims and their upstream ISP networks if backpressure is used	Protocols between detection systems
8. Computation requirement	Low	Moderate	Low	High
9. Deployment difficulty	Very high	High	Moderate without backpressure mechanisms	High
10. Technical complexity	Low	High	Moderate without backpressure mechanisms	High

Simulations by Lau etal.

Simplified version of DDoS on a single targeted router

Aim

- to compare the ability of various queuing algorithms to alleviate DDoS attacks and provide desired service to legitimate users

Single target router

- 1 Mbps bandwidth

All network links

- 1 Mbps bandwidth
- 100 ms delay

Legitimate user

- 500 byte UDP packets
- 0.1 Mbps rate

Attack daemons

- 500 byte UDP packets
- 0.3 to 1.0 Mbps rate
- Constant Bit rate

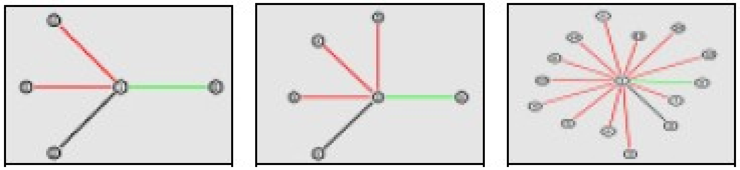


Figure 3: Simulated network topologies A, B, and C (left to right). Target is the right most node in the networks.

Performance of various Queuing Algorithms under DDoS Attack

Queuing algorithms examined

- Drop Tail
- Fair Queuing
- Stochastic Fair Queuing
- Deficit Round Robin
- RED
- Class Based Queuing

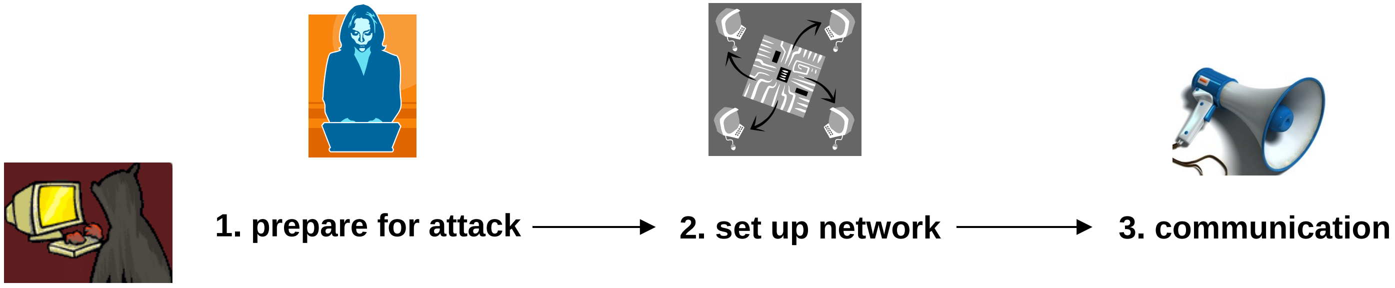
Conclusions

- Except for RED & Class based Queuing no other algorithm could guarantee bandwidth during DDoS attack
- RED provides limited bandwidth
- Class based Queuing algorithm could guarantee bandwidth for certain classes of input flow, but it requires additional efforts

Appendix A

Typical DDoS Attack (Trinoo)

DDoS: Typical attack process

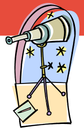


Attacker

1. prepare for attack → 2. set up network → 3. communication

www.csl.mtu.edu/cs6461/www/Slide/ddos5090.ppt

DDoS: Typical attack



The attacker prepares
scanning tools,
attack tools,
root kits,
daemon and master programs,
lists of vulnerable hosts
and previously compromised hosts

Attacker scans large ranges of network blocks to identify potential targets. Targets would include systems running various services known to have remotely exploitable features

A list of vulnerable systems is then used to create a script that performs the exploit, sets up a command shell to confirm the success of the exploit. The result is a list of "owned" systems ready for setting up back door, sniffers, or the daemons or masters

http://staff.washington.edu/dittrich/misc/trinoo.analysis

DDoS: Typical attack (contd..)

- □ A script is then run which takes this list of "owned" systems and produces yet another script to automate the installation process
- □ The result of this automation is the ability for attackers to set up the denial of service network, on widely dispersed systems whose true owners are unaware of it and these systems go out of their control, in a very short time frame
- □ Optionally, a "root kit" is installed on the system to hide the presence of programs, files, and network connections
- □ The attacker(s) control one or more "master" servers, each of which can control many "daemons“
- □ The daemons are all instructed to coordinate a packet based attack against one or more victim systems
- □ All that is then needed is the ability to establish a connection to the master hosts to be able to wage massive, coordinated, denial of service attacks

http://staff.washington.edu/dittrich/misc/trinoo.analysis

End!

At last!