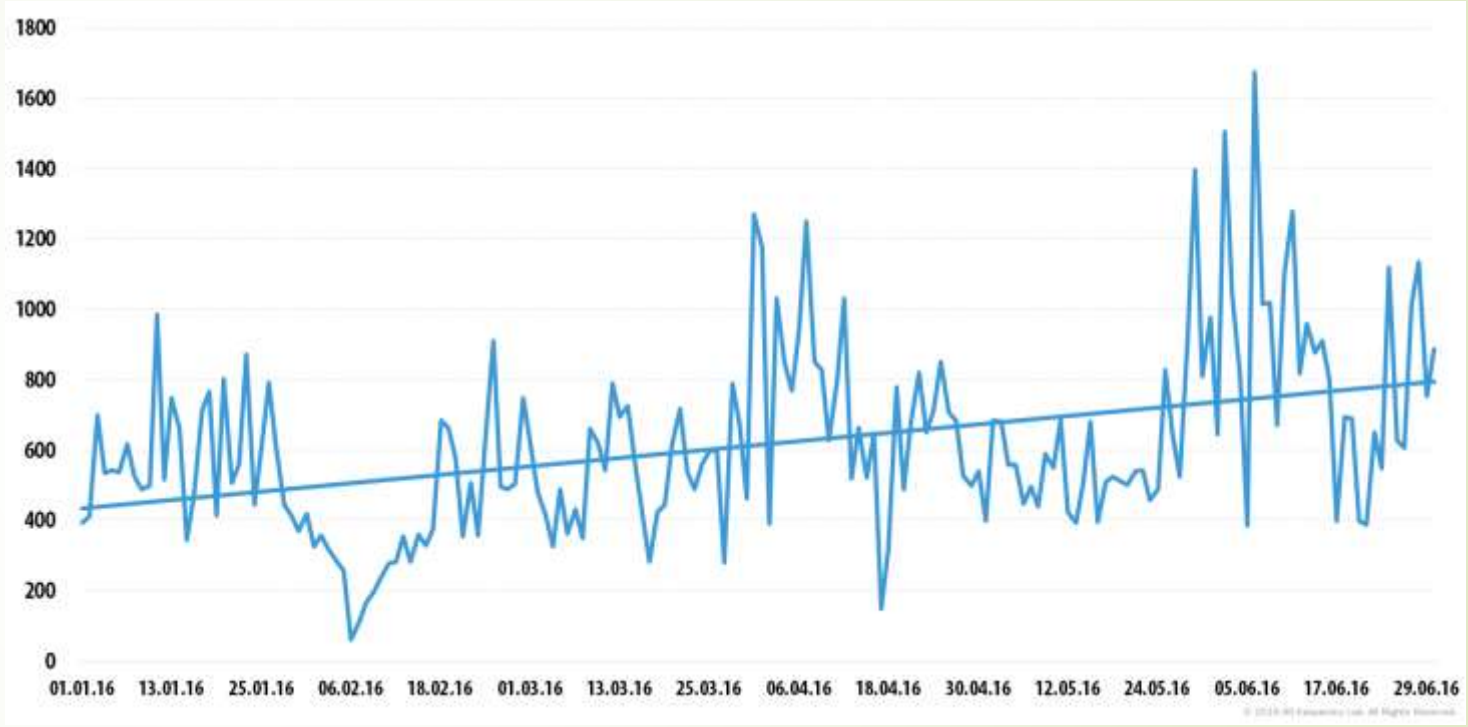
DDoS:
Attack and Defense

by: Subo Zhuang

University of Rochester

What is DoS and DDoS?

- DoS
  - a.k.a. Denial of Service attack is an attack by a single person or host to cause the victim to deny service to its customers.
- DDoS
  - a.k.a. Distributed DoS, when multiple hosts attacks simultaneously
- Difference
  - DoS → Attack is one source to one destination
  - DDoS → Multiple sources to one destination
- The frequence and impact of DDoS are increasing…



Number of DDoS attacks, Q1 2016 – Q2 2016 Kaspersky Lab

Case Study: Dyn(DNS provider)

- On Friday October 21, 2016, Dyn suffered DDoS from 11:10 to 13:20 and then again from 15:50 until 17:00.
- Causing major sites including Twitter, Reddit, GitHub, Amazon.com, Netflix, Spotify and Dyn's own website, to become unreachable.
- Official report on this:
  - The Friday October 21, 2016 attack has been analyzed as a complex & sophisticated attack, using maliciously targeted, masked TCP and UDP traffic over port 53.
  - Dyn confirms Mirai botnet as primary source of malicious attack traffic.
  - Attack generated compounding recursive DNS retry traffic, further exacerbating its impact.

About Mirai

- Devices infected by Mirai continuously scan other Internet of things (IoT) devices.
- Mirai identifies vulnerable IoT devices using a table of more than 60 common factory default usernames and passwords, and logs into them to infect.
- Infected devices will continue to function normally, except for occasional sluggishness, and an increased use of bandwidth.
- A device remains infected until it is rebooted. After a reboot, unless the login password is changed immediately, the device will be reinfected within minutes. Upon infection Mirai will block remote administration ports.
- Once infected, the device will monitor a command and control server which indicates the target of an attack. The reason for the use of the large number of IoT devices is to bypass some anti-DoS software.

--wikipedia

More Serious Situation

- During two intervals on November 30, 2015 and December 1, 2015, several of the root name servers received up to 5 million queries per second each.
- Some root server networks became saturated, resulting in timeouts, however redundancy among the root servers prevented the DNS root service going down.
- What if the root server crash?
  - The world wide Internet could be in paralysis.
- We must know how to protect our server!
- First, let's learn how the attack is performed

DDoS Attack Prerequisites

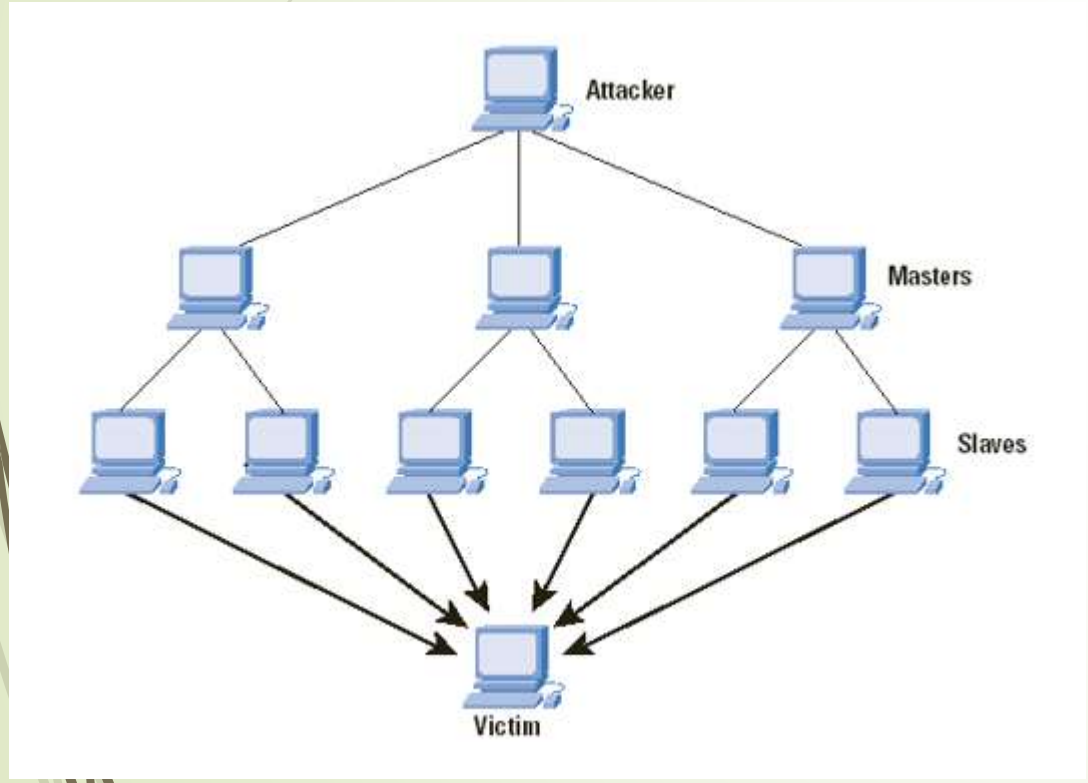
- Botnets
  - Build Botnet
    - discover vulnerable hosts
    - exploit
    - install attack tools
    - hosts become zombies or slaves.
    - many zombies together → botnet
  - Buy one.
    - many hackers sell or lease Botnet on online forum.

How DDoS Is Performed

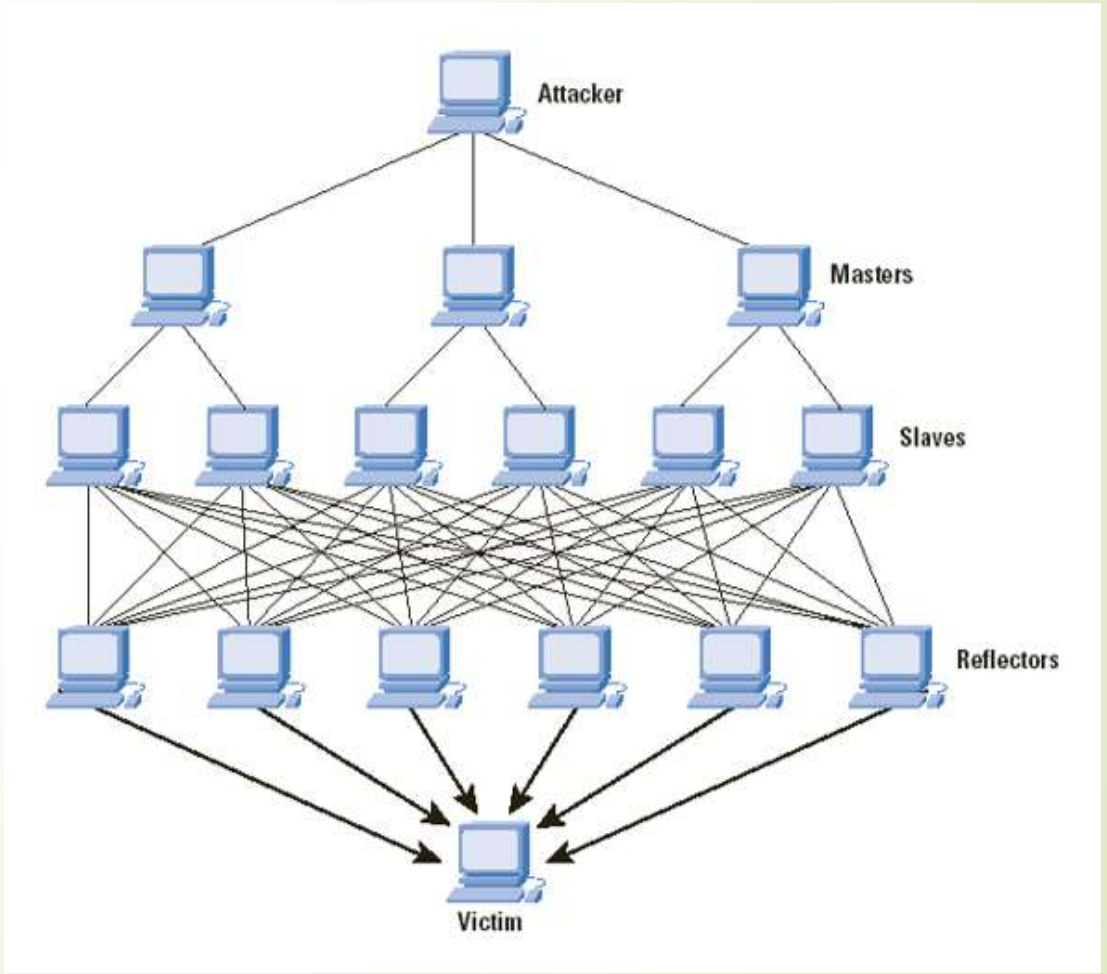
- After building the Botnet, attacker specify type of attack and victim's address
- Wait for time
  - either by remotely activating the attack to "wake up" simultaneously
  - or by programming
- The zombies begin attack
- The victim's system is flooded with useless load and exhaust its resources
- The legitimate users are denied

DDoS Attack Types

- Typical DDoS Attack

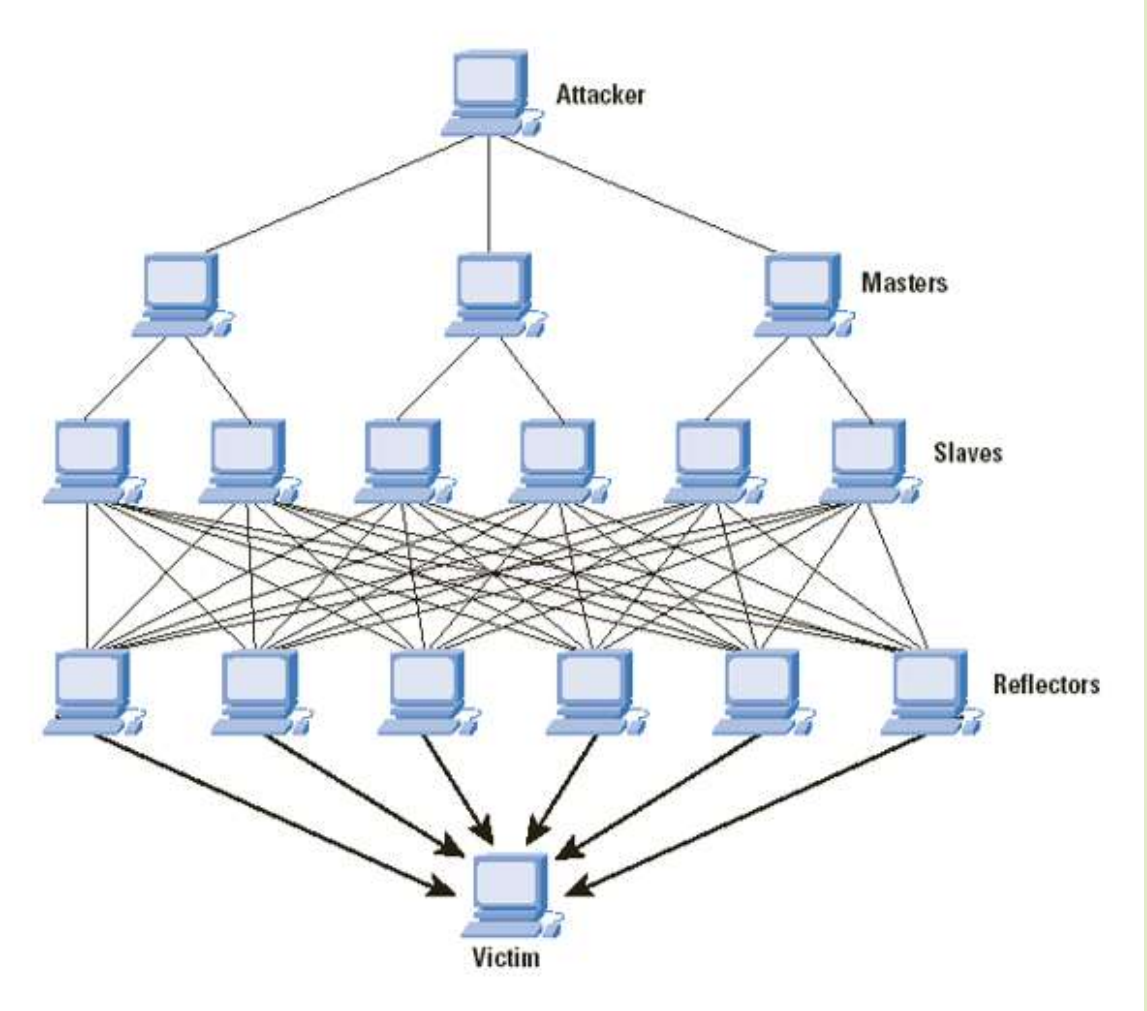


Distributed Reflector DoS Attack [1]



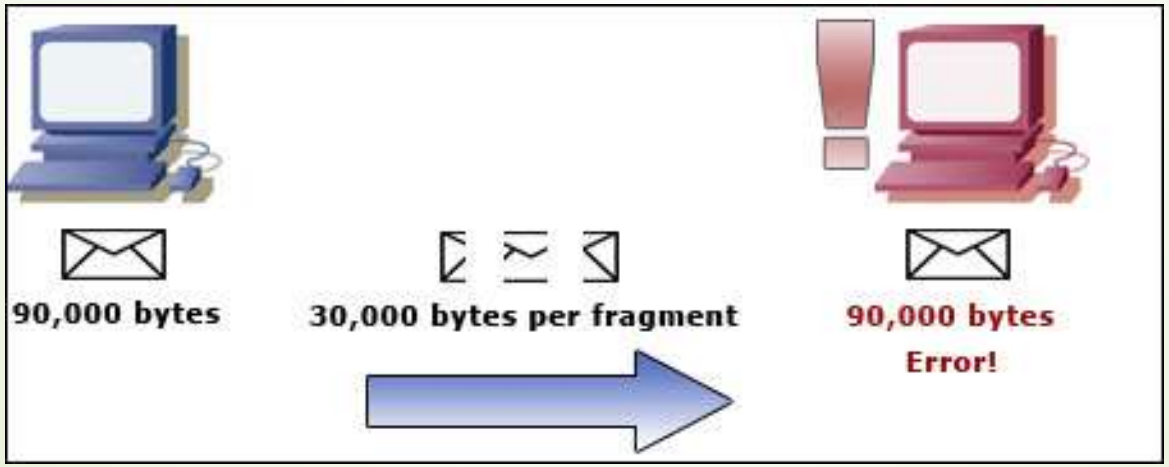
DDoS Attack Types

- Distributed Reflector DoS Attacks:
  - Send packets with the victim's IP to the uninfected machines (reflectors).
  - The reflectors send large volume packets to victim (because they think victim asked for it).
  - Most reflectors do not have firewall to filter the spoofed packet.
  - Even harder to track the attacker. [1]



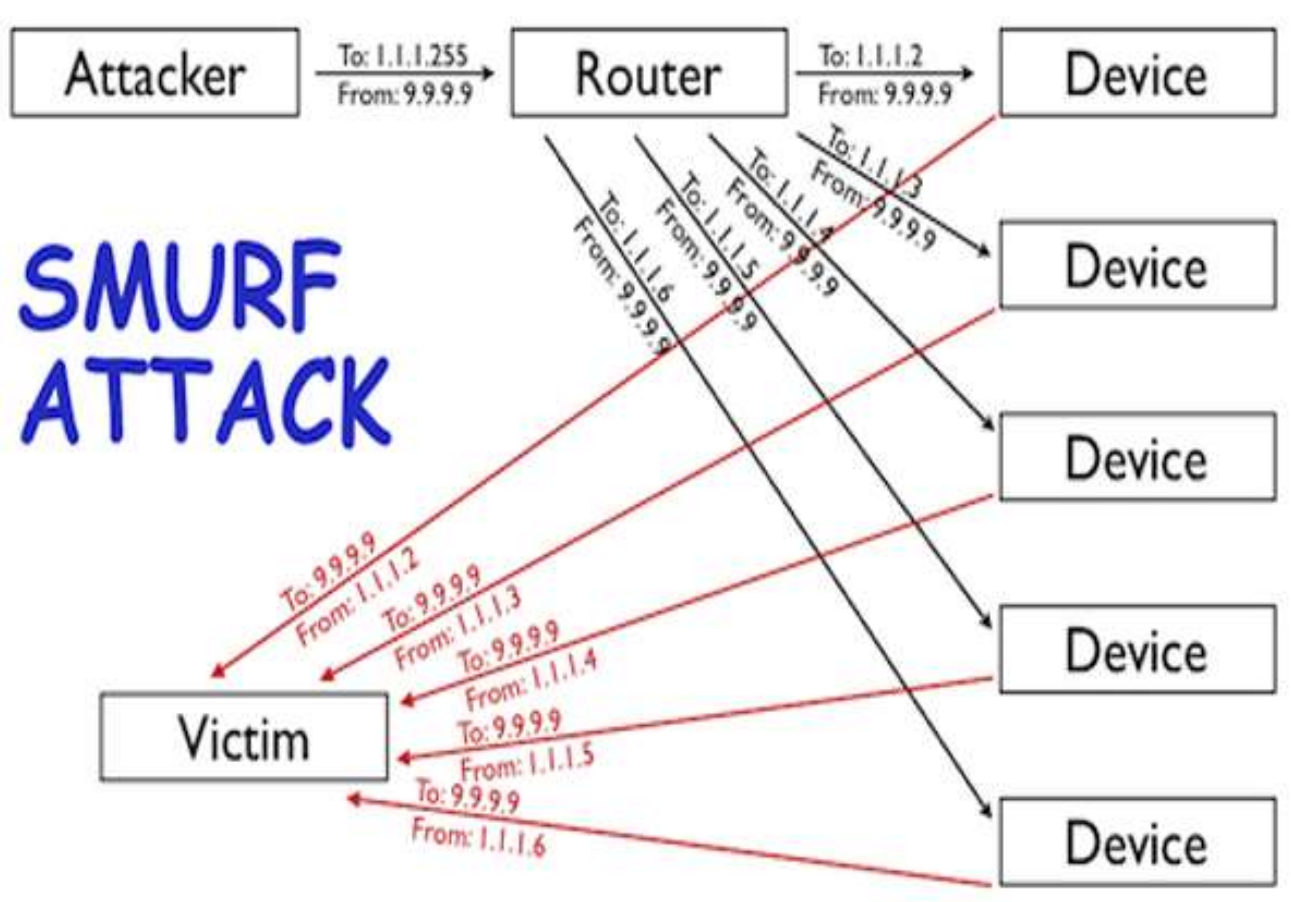
Famous DDoS Attacks

- Ping of Death
  - Infected host send a ping request that is larger than 65,536 bytes. The IP protocol allows the packet to be fragmented.
  - The victim would assemble the ping request packet in buffer, which cause the buffer overloaded even crashing the system.[2]



Famous DDoS Attacks

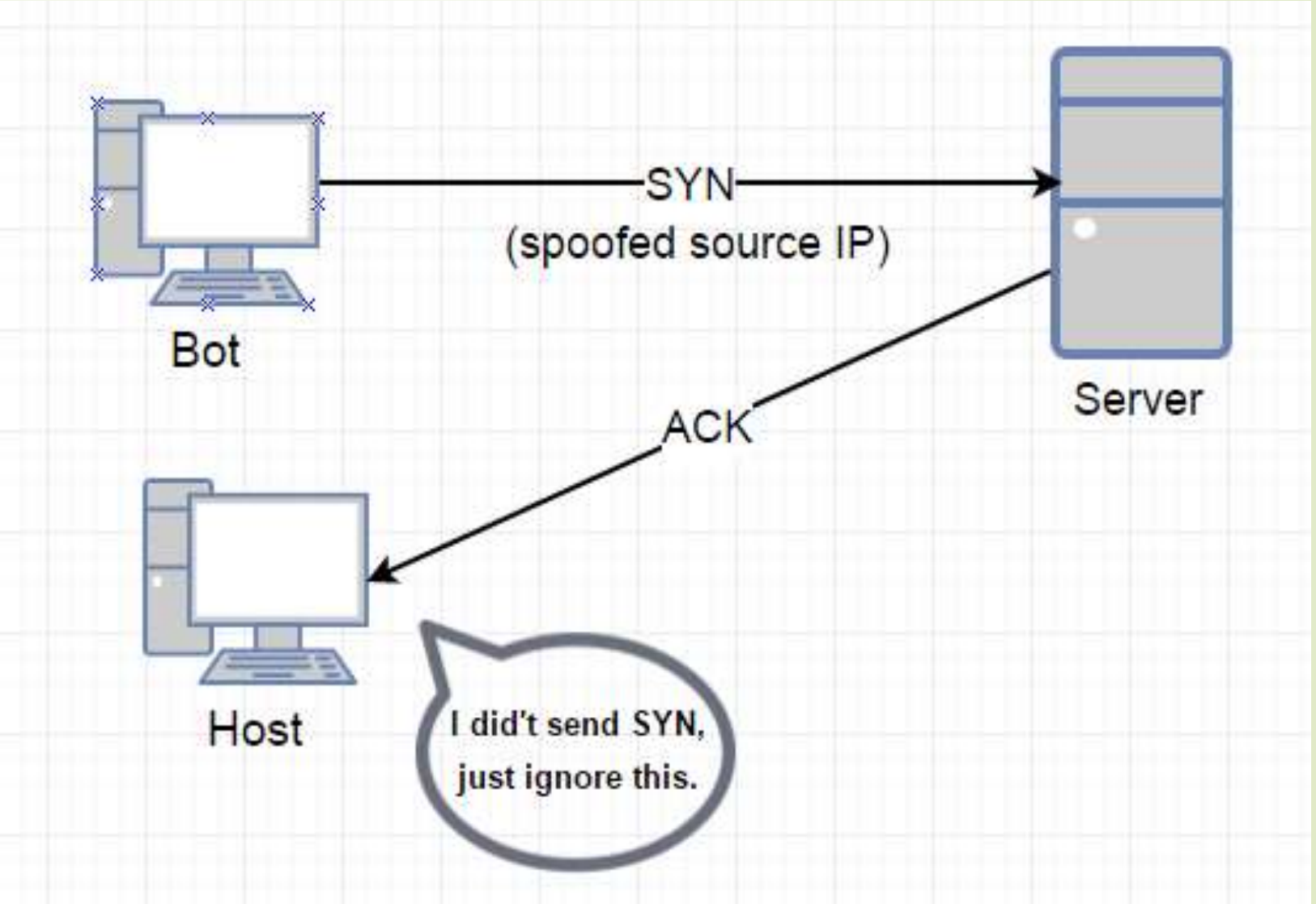
- **Smurf Attack**
  - IP address of the victim is obtained by the slaves.
  - Broadcast ICMP messages with victim's IP.
  - All the devices in this network get these ICMP messages and they send back ICMP replies to the IP address of the victim.
  - Victim get flooded with packets coming from all these uninfected hosts and crashes.[3]



--Distributed Denial of Service Attacks And Defense mechanisms, Ashish Raghupatruni

Famous DDoS Attacks

- **SYN FLOOD**
  - The zombies send abundance of TCP SYN.
  - Obliging it both to open a lot of TCP connections and to respond to them.
  - Victim unable to accept any new incoming connections, because its queue is full of half-open TCP connections.[1]



DDoS Attack Defense

- Unfortunately, there is no fail-safe solution available unless all devices cannot be infected.

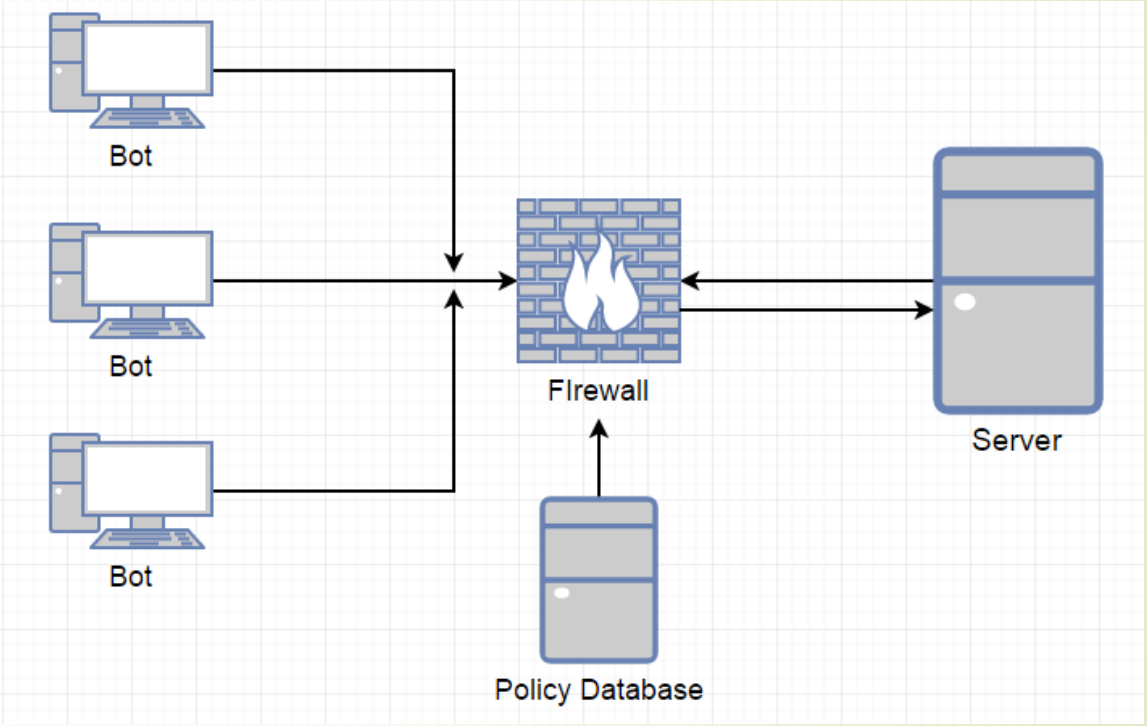
- Difficulties
  - Any attempt of filtering the incoming flow means that legitimate traffic will also be rejected.
  - Attack packets usually have spoofed IP addresses which makes it difficult to traceback the source of attack.
  - There is the danger of characterizing a legitimate connection as an attack .[1]

DDoS Attack Defense

- Add More Servers
  - Resource competition-- essential issue of DDoS.
  - If a defender has sufficient resources to counter a DDoS attack, then the attack will be unsuccessful, and vice versa.
  - Effective but costly.
  - Not a good solution to DDoS. -- What if the botnet get bigger and bigger?

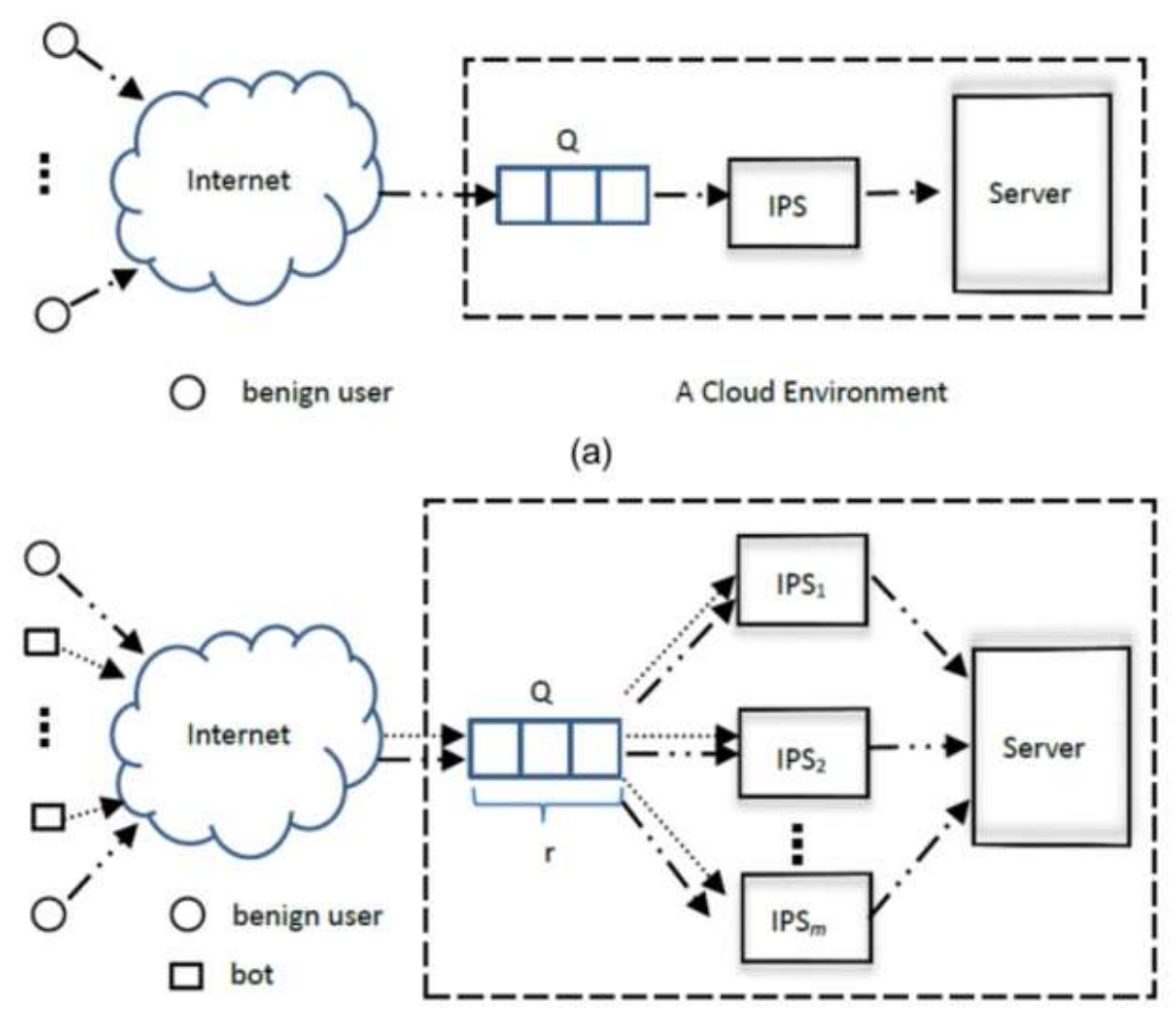
DDoS Attack Defense

- Route Filter
  - Routing suspicious traffic to a valid IP address where it can be analyzed.
  - Traffic that is found to be malicious is rejected.
  - Again, legitimate traffic from user could also be rejected.
  - And the attack methods could be various. Take enormous effort to build a good Firewall.



DDoS Attack Defense

- DDoS Attack Mitigation in Clouds[4]
  - When the DDoS attack happens, the clouds can redirect the request to one of these IPSs to be filtered, and only the clean traffic will go to server
  - Sites have the ability to handle massive amounts of bandwidth and have DDoS mitigation capabilities
  - most cost effective and reliable means of protecting servers



IPS: Intrusion Prevention System

Summary

- Attacker Use botnet to perform attack.
- It a competition of resources.
- As the number of IoT things grows faster, the threaten of DDoS is also growing.
- Clouds provide a cost effective and reliable way to mitigate DDoS attack.

Thank you !

Refrence:

[1] Jignesh Patel, DDoS Attacks, http://www.slideshare.net/jignesh/ddos-attacks, 2006.

[2] Kaustubh Padwad, Denial of service Attack, http://www.slideshare.net/kingkaustubh1/denial-of-service-attack, 2015.

[3] Ashish Raghupatruni, Distributed Denial of Service Attacks And Defense mechanisms, http://www.slideshare.net/AshishRaghupatruni/ddos-ppt, 2016.

[4] S. Yu, Y. Tian, S. Guo and D. O. Wu. Can we beat DDoS attacks in clouds? IEEE Transactions on Parallel and Distributed Systems 25(9), pp. 2245-2254. 2014. . DOI: 10.1109/TPDS.2013.181.

[5] R. Heinrich. DDoS attacks: Detecting attacks and defending the network. ProQuest Dissertations and Theses pp. 60. 2015. Available: http://search.proquest.com.ezp.lib.rochester.edu/docview/1719458657?accountid=13567.