A Contemporary Survey and Taxonomy of the Distributed Denial-of- Service Attack in Server

B.Hemalatha[#1], Dr.N.Sumathi[#2]
#1 Research Scholar, Department of Information Technology,Ramakrishna College of Arts and Science, Coimbatore,Tamil Nadu, India
#2 Head ,Department of Information Technology,Ramakrishna College of Arts and Science, Coimbatore,Tamil Nadu, India

Abstract

Distributed Denial-of-service (DDoS) attack is one of the most perilous threats that could cause overwhelming effects on the web. The name entails, it's an attack with the purpose of denying service to legitimate users, Distributed Denial of Service (DDoS) is defined as an attack in which several conciliation systems are made to attack and make the targeted systems services unavailable, this attack deliberately designed to render a system or network incapable of providing normal services. DDoS attack affects the computing environment, communication and server resources such as connectivity sockets, processing elements, memory, data bandwidth, network routing process etc for mutually connected system environment would surely vulnerable to the entire computing environment. It becomes essential for researchers and program developers to understand the behavior of DDoS attack because it has an effect on the target network without warning. Therefore must to develop an advanced intrusion detection and prevention systems for detecting and preventing to DDoS attack in the cyber space.

This survey and taxonomy paper deals with the introduction of DDoS attacks, DDoS attack history and recent occurrence, DDoS attack tactics, different DDoS attack tools, and taxonomy of various attack and preventive mechanisms.

Keywords: *DDoS attack, Types of DDoS, preventive measures of DDoS, defense technique, security*

I. INTRODUCTION

Distributed Denial of Service attacks started in the year 1998 but the persuade of it was become conscious by the people, corporate and IT segment were feel on DDoS attacks in the time of July 1999. The several types of DDoS attack tools such as Trinoo, Low Orbit Ion Cannon LOIC, High Orbit Ion Cannon (HOIC), tool hping, Slowloris, Tribe flood network (TFN), R U Dead Yet? (R.U.D.Y.), Shaft, and Stacheldraht are identified and examined. All the above tools could instigate DDoS attacks from number of compromised host and take down virtually any connection, any network on the Internet or web by just a little command keystrokes.

DDoS attack works in different faces like flooding attack or SYN flooding attack, logic attack and protocol-based attack.

(a)Flooding attack or SYN flooding attack is an attack in which it sends unwanted malicious packets to the network, i.e. either the node may send duplicated packets or the node systems may send the unique packets which exceed its appropriate limit.

(b)Logic attack is an attack which has a buffer memory space limit and it may exceed or overflow when it accepts a huge volume of packets beyond its limit.

(c)In protocol-based attack intruder does not weakens the TCP/IP protocol function in its place it take the expected behavior of this protocol for the requirements of attacker.

On 21 October 2016, a distributed denial of service (DDoS) attacks involving millions of Internet Protocol (IP) addresses had been marked and attacked Domain Name System (DNS).The enormity of the attack was claimed to be 1.2 Tbps and it also involved Internet of Things (IoT) devices. This noteworthy incident of DDoS attacks has confirmed the immense danger intrinsic with DDoS attacks and has taken the more attention in the computing society.

The recent Kaspersky statistics figure: 1 and figure: 2 show the DDoS is more malicious then other vulnerability.

The severely affected countries and the types of DDoS attacks

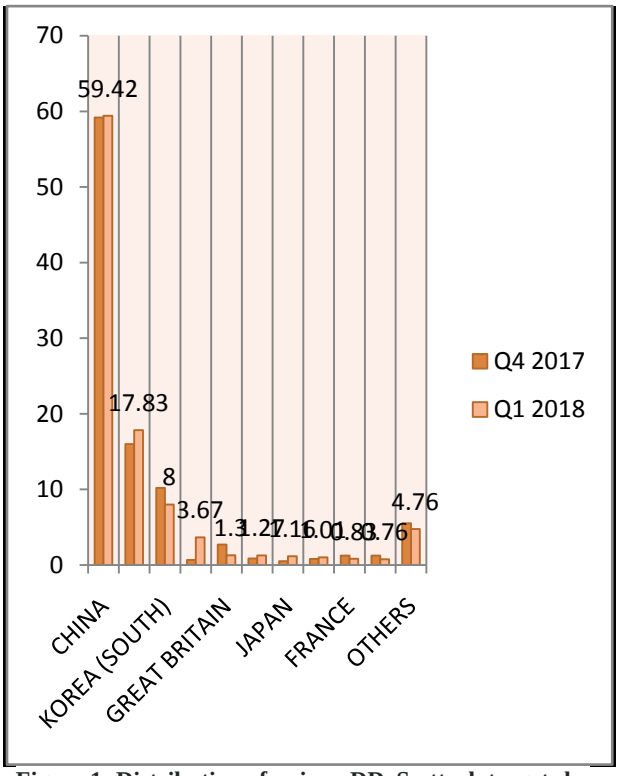

Figure 1: Distribution of unique DDoS-attack targets by country, Q4 2017 and Q1 2018

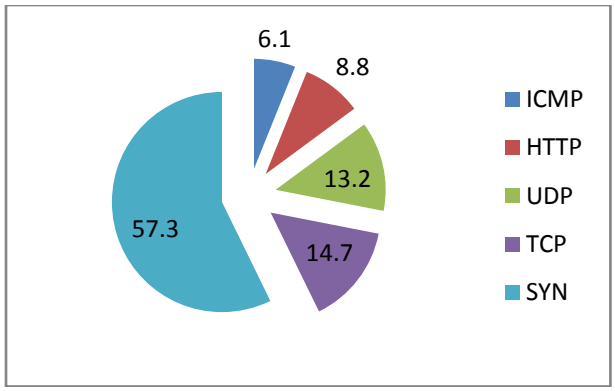

Figure 2: Distribution of DDoS attacks by type, Q1 2018

II. TYPES OF DDOS ATTACK

DDoS attacks[2] are classified into two types they are major types and common types, the three major types of DDoS attacks are:

A. Volumetric attacks or **Volume Based Attacks**

Includes UDP floods, ICMP floods and other spoofed packet floods which sends the flood of spoofed packet to the network and it affect the bandwidth of a website, server and bring legitimate traffic to crawl and enormity is measured in bits per second (Bps).

B. Protocol attacks

like SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more. This type of vulnerability consumes more server resources, intermediate communication equipments(like firewalls, monitoring tools and load balancers), and it is measured in packets per second (Pps).

C. Application layer attacks

like Slowloris, GET/POST flooding attack, attacks that target web server, and OpenBSD and more vulnerabilities which are made up of apparently legitimate requests to applications and services, but in magnitude designed to overwhelm the server and is measured in Requests per second (Rps).

D. The fifteen common types of DDoS attacks are [21]

1. DNS amplification

attack [3] is a reflection-based DDos attack. The attacker spoofs the look-up requests to domain name servers to hide the source of the exploit and direct the reply to the target system.

2. UDP Flood

In this type of attack, the attacker uses UDP datagram protocol; it contains IP packets to overflow random ports on a target network. The victimized system attempts to go with each datagram in an application, but it fails. The system immediately overwhelmed and it tries to handle the UDP packet responds volume.

3. DNS Flood

alike to UDP flood, this type of attack involves attacker using huge volume of UDP packets to exhaust server side resources. Here, however, the target is Domain Name Servers and their cache memory, with the aim being to prevent the redirection of legitimate incoming requests to the DNS.

4. HTTP Flood

attack uses a tremendously huge volume of HTTP GET/ POST requests, apparently legitimate to the target application or web server. These requests are repeatedly crafted to avoid detection with the executor, and get useful information prior to the attack.

5. IP Fragmentation Attack

involves perpetrators utilize an IP datagram's Maximum Transmission Unit (MTU) overload to a system. This can be done by sending fake ICMP and

UDP packets that surpass the network MTU to the point where resources expend quickly and make the system unavailable at the time of packet reconstruction.

6. NTP Amplification

is held at Internet-connected devices use Network Time Protocol (NTP) servers for clock synchronization. It similar to a DNS amplification attack, here a attacker uses a number of NTP servers to overload a target system with User Datagram Protocol (UDP) traffic.

7. Ping Flood

is a common flood-type of attack that uses surplus of ICMP echo requests, or pings to the victim's network. For every ping it sent a reciprocal one containing the same number of packets is supposed to be returned back to the origin. The targeted system tries to respond to the numerous requests, finally congestion on its own network bandwidth.

8. SNMP Reflection

Simple Network Management Protocol (SNMP) enables system administrator to configure remotely and drag the data from connected network devices. Using a victim's forged IP address; an attacker can explode a lot of SNMP requests to devices, each request is expected to reply in the turn. The number of connected devices gets sending upward, with the network finally being throttled by the large amount of SNMP responses.

9. SYN Flood

attack held at TCP session, it requires a three-way handshake protocol works between the two systems involved. Using a SYN flood, an attacker quickly hits the target system with lot of connection requests that it cannot keep up, and it leading to network diffusion.

10. Smurf Attack

acts like a ping flood attack, it relies a huge collection of ICMP echo request packets. But the similarity stops there, as a smurf attack uses an amplification factor to increase their payload potential on the broadcast networks.

11. Ping of Death

is a form of attack is used by the hackers to send abnormal or inflated packets to freeze the victim system and destabilize or crash a targeted system or service. In this attack Memory overflow occurs when it tries to reconstruct the oversized data packets.

12. Fork Bomb

attack originates within the target server. In a UNIX operating system, a fork system call copies an existing process to a next process. Both the processes can tackle concurrent tasks in the system kernel independent of one another. Using a fork bomb a attacker issues number of recursive forks to the targeted system it becomes internally overwhelmed.

13. Mail Bomb

is another type of bandwidth-based flood attack. A mail bomb attack method is sending of an enormous amount of e-mail to a particular person or system. A massive amount of mail may fill up the victim's disk space on the server or, in some time, it may be stop the server function.

14. IGMP Attack

is snooping process of eavesdropping to Internet Group Management Protocol (**IGMP**) network traffic. It allows listening in the network conversation between hosts and routers in this attack, flooding the network with randomly passing IGMP messages. It makes overload on the network and reduced broadband and memory usage.

15. SQL Slammer

is a type of computer worm it causes the Denial of Service on some internet host, severely it slow down the internet traffic. It exploits the buffer overflow vulnerability in SQL database server.

E. DDoS attack strategies

The basic structure of a DDoS attack comprises three different phases figure: 4 and three different components figure 3. The tools or components are known as an attacker, multiple control masters or handlers, multiple slaves, agents, or zombies, and a victim or target machine.

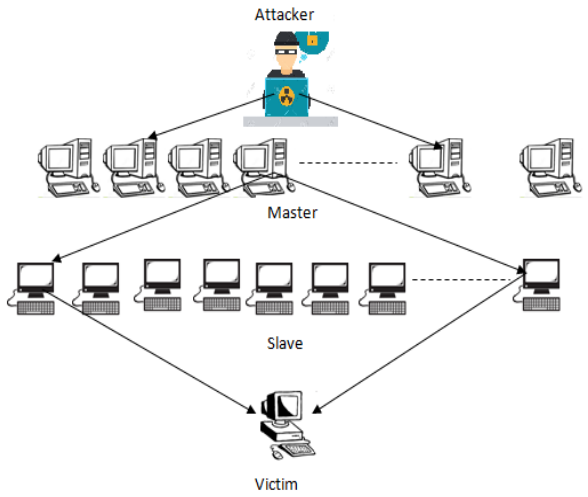

Figure 3: Structure of a DDoS attack.

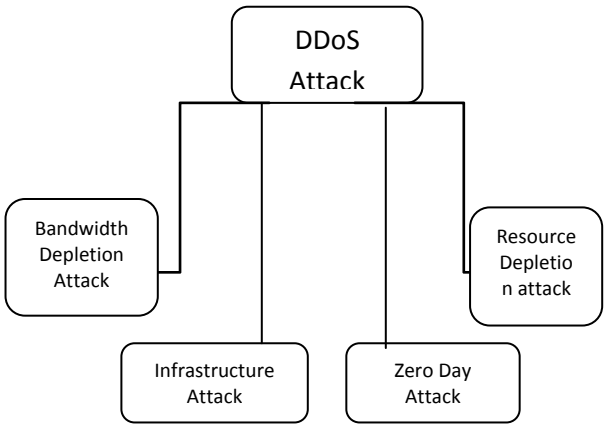

Figure 4: Different types of DDoS attacks

In the first phase, the attacker spends a lot of its time to create a significant amount of compromised systems which are called the masters or handlers as they appoint and control the other systems in the attack. The formation of the master systems is usually an automated process where a incessant scanning is performed to look for systems with security loopholes. The malicious codes installed by the attacker into this master systems further to add more infected machines into the attack. The slave machines are directly controlled by the masters systems and indirectly controlled by the attacker through these masters systems.

The second phase starts if an adequate number of devices have joined as a compromised system. This compromised system is known as botnets. In this phase, the attacker moves all necessary information like codes and commands to the master systems which in turn to send those to all slave systems to get prepared for the attack.

In the third phase, the attacker commands to the top controlled systems to start and execute attacks. Thus, it attacks the victim in a distributed method and sends a large volume of packets which in turn flood the victim's systems. In these type of attacks, the attacker habitually uses spoofed IP addresses which helps attacker to hide the identity of the compromised devices.

F. Attack based on degree of mechanization[23]

Attack based on different phases and characteristics it can be manually set, controlled by the attacker, or may be automated. Therefore, there are three different types of attack set-ups: manual, semi-automatic, and automatic.

1. Manual

In this type of attack, the attacker does all of the works manually. The scanning of the machines to find the security loopholes and controlling the compromised systems are performed in a manually. This type of scenario seen in early days. Today, all of the actions have become systematically automated and made DDoS attacks easier.

2. Semi-automatic

In semi-automatic method, the communications between the handler and the agents are to some extent manual as they communicate to know each other. Based on the directions and commands received from the attacker they set the method, the duration of time, and the victim of the attack. However scanning, recruiting, and compromising the handler's systems are automatic in this attack scenario.

3. Automatic

In this attack method, all of the phases and needs are implemented automatically. Here, the attacker attacks a victim system without any communication with handlers or any other agents. All the requirements of the attack systems are coded in the attack code which is installed in the compromised systems and later executed to perform an attack.

III. NEED FOR DDoS DEFENSE MECHANISM

In DDoS defense system is basically traffic monitoring, traffic analysis, traffic filtering mechanism. Defense mechanism can be applied in two ways they are centralized and distributed. In a centralized system all components are placed at same location. It is extremely vulnerable to attack. There is no cooperation with other communication modules because it consists of minimum number of resources are available for defense against DDoS attack.

In distributed system components are placed at different places and it is less vulnerable to attack, it cooperated with the entire communication modules, so the complete systems is in a proper communication framework. More resources are available for protecting against the vulnerability. It deployed all over the network .The centralized defense mechanism only concentrated and monitoring on the victim's node. But distributed system can find any attacker node in the network.

IV. GENERAL TECHNIQUES

There are several solutions existing for DDoS defense, they do not give a complete protection against DDoS attacks in a single point solutions**.**

A. Disabling unused

there are number of applications and open ports in hosts, the less there are chance to exploit vulnerabilities by attackers. Therefore, if network

services are no needed or unused, the services should be render inoperative to prevent attacks

B. Install latest security patches

many DDoS attacks exploit vulnerabilities in target systems. So fixing known security loopholes by installing all relevant latest updated security patches prevents re-exploitation of vulnerabilities in the target system

C. Disabling IP broadcast

Defense against DDoS attacks that use intermediate broadcasting nodes e.g. ICMP flood attacks, Smurf attacks etc. It will be successful only if host computers and all the neighboring networks disable IP broadcast

D. Firewalls

can efficiently prevent users from launching flooding attacks from machines behind the firewall. Firewalls, rules such as to allow or deny protocols, ports or IP addresses. But some complex attack e.g. if there is an attack on port 80 (web service), firewalls cannot prevent that attack because they cannot differentiate good traffic from DoS attack traffic

E. Global defense infrastructure

can protect from many DDoS attacks by installing filters in the routers of the network. The network is administered by various autonomous systems according to their own local security policies.

F. IP hopping

can be prevented by changing the network location or IP address of the active server proactively within a pool of homogeneous servers or with a marked set of IP address ranges. The victim systems IP address is invalidated by changing it with a new IP. Once the IP addresses change is completed all internet routers will be informed and edge routers will filter and drop the attacking packets.

V. DEFENSE PRINCIPLES of DDoS

Some existing defense solutions for DDoS is given below

A. Rate Limiting Mechanism

The rate limiting mechanism that limits the rate of the packet arrived, which contented the criteria for DDoS attack. This rate limit mechanism only limits the rate of malicious packet. That does not harm legitimate flow of packet. It does not acquire lot of the overhead. It is the simple form of the packet filtering.

B. Egress/Ingress Mechanism

these two types of filtering make it difficult for attackers to launch attack using spoofed IP address. IP spoofing makes it very difficult to trace back the attack to actual originating host. Ingress filtering method is proposed by **Ferguson et al**. is a restrictive mechanism to drop the traffic with IP addresses that do not match a domain prefix connected to the ingress router. Egress filtering is an outbound filter, which ensures that only assigned or allocated IP address space leaves the network. A basic requirement for ingress or egress filtering is expected IP addresses at a particular port.

C. Source Address Validity Enforcement

(SAVE) protocol enforces the routers to send messages containing updated source information to each destination routers connected to a source. Then, every router updates its forwarding table with present information and uses it to filter the packets based on the RPF.

D. Three-Way Handshake

method is used to defense source spoofing at the end system. It will inadequate to finish when source host spoofs its IP address. But attacker can spoof the source IP address of first packet of the three-way handshake.

E. Path identifier

method is used to filter outs packets based on a path identifier that identifies the path of the attacker.

F. Martian address

filtering techniques and source address validation is defined in RFC 1812 and it works for filtering spoofed IP addresses that are created from a limited set of addresses. This filtering technique ensures that a router should not forward any packet which has an invalid source or destination IP address.

Commonly used current defense techniques' in the DDoS

G. Route-based packet filtering

(RPF) technique filters packets with spoofed source IP addresses. This filtering method increases the possibility of the Ingress filtering by providing service to the core routers.

H. Hop Count Filtering

technique use spoofed IP Packet at the beginning of network processing by using a hop-count filtering mapping table. Using the table it can easily identify the spoofed IP address. In this method, the authors have used the concept that it is not possible to change the number of hops of an IP packet when it travels from the source to a destination.

I. History-based filtering

this is another way of packet marking based filtering mechanism where the history of the normal traffic is used to filter out the malicious attacks

j. Trace back

is the process of tracing back the fabricated IP packet to valid source rather than Spoofed IP address that was used by attacker. There are three methods to doing trackback (i)Link testing scheme (ii)ICMP trace back message .(iii)packet marketing scheme.

K. Packet Score method

is a proactive filtering technique which uses Bayes' theorem to calculate the conditional legitimate probability (CLP). This CLP is used to find out the likelihood of a genuine packet
based on the baseline value and the attribute value of the packet.

Table 1: Comparison of DDoS prevention

Tools used for process	Pros	Cons
Route based Packet filtering	Works Well with static routing	Problem when dynamic routing is used Needs wide implementation to be effective
Hop Count Filtering	Hop-Count Filtering (HCF) constructs an exact IP to Hop-Count (IP2HC) mapping table to detect and remove spoofed IP packet	Need a systematic approach for setting up the parameters of HCF, such as the occurrence of dynamic updates and efficiency of HCF against the simulated actual attacks from real attacks
History based filtering	Does not require cooperation of whole internet community Gives priority to frequent packets in case of congestion or attack	In effective when the attacks come from real IP addresses Require an offline database to keep track of IP address Depend on information collected
Trace back	Identifies spoofed sources of attacks	Router Overhead
Packet Score method	The incoming packets are allocates a scores based on the priority coupled with the attributes and on association with probability distribution of incoming packets on per packet basis.	Some feedback delays in a distributed implementation and in the network processors

VI. CONCLUSION

DDoS attack is one of the recent and advanced attacking technique in network system, it protects legitimate user from using network resources. In this paper major contributions are a need of Distributed DoS defense mechanism and its evaluation. While developing a DDoS defense system, the issues are discussed in this paper need to be deliberated and considered with due seriousness. In this research survey paper, we have presented an overview of different types of DDoS attacks, attack detection schemes and finally research issues and challenges. In addition, we provide a comparison between the existing and current detection methods. This paper illustrated a comprehensive survey of causes of DDoS attack and its defense mechanism. According to this survey most of the defense approach had used to rate limiting mechanism. Egress and Ingress method had used in defense against IP spoofing. Each method has some special features that make it more appropriate to implement in one situation than another.

REFERENCES

[1] Abdulkader A. Alfantookh "DoS Attacks Intelligent Detection using Neural Networks" J. King Saud University, Vol. 18, Computer & Information Science., pp. 27-45 A.H. 1426/2006

[2] Rufaikazeem Idowu, Ravie chandren M. Zulaiha ali othman "Denial of service attack detection using trapezoidal fuzzy reasoning spiking neural p system" Journal of Theoretical and Applied Information Technology, 31-5-2015. Vol.75. -No.3

[3] https://www.us-cert.gov/ncas/alerts/ TA13-088A

[4] MaryamM.Najafabadi, TaghiM. Khoshgoftaar, AmriNapolitano, Charles Wheelus "RUDY Attack : Detection at the Network Level and Its Important Features" Proceedings of the 29th International Florida Artificial Intelligence Research Society Conference

[5] X.Geng, A.B.Whinston, "Defeating Distributed Denial of Service attacks", IEEE IT Professional 2-4-2000 page no. 36–42.

[6] FelixLau, RubinH.Stuart, SmithH. Michael, and et al., "Distributed Denial of Service Attacks," in Proceedings of 2000 IEEE International Conference on Systems, Man and Cybernetics, Nashville, TN, Vol.No.3, pp.2275-2280, 2000.

[7] Alagarsamy, Vadivel MuruganP. "Averting Buffer Overflow Attack in Networking OS using - BOAT Controller" International Journal of Computer Trends & Technology, July 7, 2013, volume 4

[8] P.Ferguson, and D. Senie, "Network ingress filtering: Defeating denial of ser-vice attacks which employ IP source address spoofing" RFC 2267, the Internet Engineering Task Force (IETF), 1998),

[9] R.Oppliger, "Internet Security: firewall and beyond," Communications of the ACM, Volume 40, Issue 5, pp. 92-102, 1997.

[10] P.Vadivel Murugan and Dr.K.Alagarsamy " Buffer Overflow Attack Vulnerability in Stack". International Journal of Computer Applications 13(5)

[11] S.A.Arunmozhi, Y.Venkataramani, "DDoS attack and Defense in wireless ad-hoc Network," International Journal of Network Security & Its Applications Vol.3, No.3, pp.182-187, May 2011

[12] York, K. Dyn statement on 10/21/2016 DDoS ttack, 2017, http://dyn.com/blog/dyn-statement-on-10212016-ddos- attack/ (accessed 10 March 2017)
[13] www.securelist.com/ddos-report-in-q1-2018/85373
[14] M.Duraipandian and C. Palanisamy. "An intelligent agent based defense architecture for ddos attacks". In Electronics and Communication Systems (ICECS), 2014 International Conference on, pages 1–7, Feb 2014.
[15] Vadivelmurugan, p., & Alagarsamy, K. "Securing Server System from Buffer Overflow vulnerability using Vel-Alagar Algorithm. International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013
[16] https://www.eecs.umich.edu/techreports/cse/2003/CSE-TR-473-03.
[17] Jelena Mirkovic, Peter Reiher "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms" ACM SIGCOMM Computer Communications Review , Volume 34, Number 2: April 2004
[18] McAfee, "Personal Firewall". Available at: http://www.mcafee.com/ myapps/ firewall/ov_firewall.asp.
[19] Cybernetics, Nashville, TN, Vol.3, pp.2275-2280, 2000.
[20] Saman Taghavi Zargar, James Joshi, and David Tippe, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks" IEEE Communications Surveys & Tutorials
[21] Sunny Behal, Krishan Kumar "Characterization and Comparison of DDoS Attack Tools and Track Generators - A Review" International Journal of Network Security, Vol.19, No.3, PP.383-393, May 2017
[22] Lovepreet Kaur Somal, IIKaranpreet Singh Virk "Classification of Distributed Denial of Service Attacks - Architecture, Taxonomy and Tools" International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)
[23] Jelena Mirkovic, Janice Martin and Peter Reiher "A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms" Computer Science Department, University of California, Los Angeles Technical report #020018