CERTIFICATE

Delhi Technological University
BAWANA ROAD, DELHI-110042

Date: _____

This is to certify that project entitled "***A Throttle Based Approach to mitigate Distributed denial of Service Attacks*****"** has been completed by **Dhwani Garg** , in partial fulfilment of the requirement of Master Of Technology in Software Engineering.

This is an authentic work carried out by her under my guidance & the matter embodied in this research work has not been submitted earlier to the best of my knowledge and belief.

(Ms .ABHILASHA SHARMA)
PROJECT GUIDE
(Deptt. Of Software Engineering)
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
BAWANA ROAD, DELHI – 110042

ACKNOWLEDGEMENT

The satisfaction that accompanies successful completion of any work would be incomplete without the mention of the people who made it possible. Primarily, I would like to thank our university DTU and also other staff members for giving us the opportunity to fulfil my aspiration.

I am very thankful to my Project Guide, Ms. Abhilasha Sharma for her valuable guidance and remarkable patience in guiding my work to its fulfilment. I wish to thank my parents, parents-in-law and above all my husband for their constant encouragement that is like snow, softer which it falls and longer when it dwells upon, the deeper it sinks in mind. I will be failing in my mission if I do not thank other people who directly or indirectly helped me in the preparation of the project report. So my heart full thanks to all friends & staff of my University who supported & encouraged me in preparing this Report as best as possible.

(DHWANI GARG)
Master of Technology
(Software Engineering)
Dept. Of Computer Engineering
Delhi Technological University
BAWANA ROAD, DELHI-110042

ABSTRACT

Distributed Denial of Service (DDOS) is one of the most significant kind of security threats in the internet. Through this form of attack the available resources are engaged to such a level that it ceases to provide service to the legitimate users. Internet services have been the major victim of various forms of this attack with complete network faces sharp reduction in performance. Distributed Denial of Service Attack has recently emerged as one of the most newsworthy, if not the greatest, weaknesses of the internet. In this report an overview of the DDOS problem attack, defence principle and how the gap between the problem and the possible mitigation could be resolved through the application of queuing mechanism over optimum throttle algorithm has been proposed. Here we describe a novel framework that deals with the detection of variety of DDOS attacks by monitoring propagation of abrupt traffic changes inside the Network and then characterizes flows that carry attack traffic. Work in the Report targets a network architecture and accompanying algorithms for countering denial-of-service (DOS) attacks directed at an Internet Server. The basic mechanism is for a server under stress to install a router throttle at selected upstream routers. The throttle mechanism would be highly effective in preferentially dropping attacker traffic over good user traffic.

In this project we have aimed to propose an algorithm, which mitigates the above described Distributed denial of service attacks and tries to lessen the impact of these attacks.

PROBLEM STATEMENT

DOS/DDOS attacks clog the normal response capabilities of server/host computers, thus preventing legitimate users from accessing viable or critical data from the host. Many times the only remedy for a server in the midst of such an attack is to shut down the computer and restart it. DDOS/DOS attacks are not as sophisticated as viruses or hacker attacks but they can be just as time consuming and money wasting to the host computer. When a single computer attacks a host by flooding it with requests, this is a plain Denial of Service attack. When a series of computers are coordinated (or hijacked) to flood a single computer, this is a Distributed Denial of Service attack. Both attack methods can bring a server to its knees. One solution is to implement a quasi-bastion program that stands guard at the open ports of the host computer and examines the packets coming in. If a large number of packets are coming from the same source, the program will exclude them from coming in, as this may signal that a DOS attack is underway. If an unwarranted number of packets are coming in from many requestors in a short period of time, this could signal a DDOS attack is underway. DDOS attacks are difficult to detect in real time, therefore the role of this program is to make some heuristic assessments and determine if the packets are legitimate or not. If a bouncer program is employed at mission critical servers, then the cost o employing the software (i.e. the cost in terms of CPU cycles) and the slower access to the server's information for the client may be more productive and cost effective than having no bouncers and permitting everyone from everywhere to crash or shut down the server. This watchdog software object is called the "bouncer" which acts the same way a bouncer at nightclub would if the crowd is unmanageable or unacceptable.

LIST OF FIGURE(S)

LIST OF TABLE(S)

TABLE OF CONTENTS

Page No.