Chapter 11
Security Integration in DDoS Attack Mitigation Using Access Control Lists

Sumit Kumar Yadav
Indira Gandhi Delhi Technical University for Women, Delhi, India

Kavita Sharma
National Institute of Technology Kurukshetra, India

Arushi Arora
Indira Gandhi Delhi Technical University for Women, Delhi, India

ABSTRACT

In this article, the authors propose a DDoS mitigation system through access list-based configurations, which are deployed at the ISP (Internet Service Provider's) edge routers to prohibit DDoS attacks over ISPs' networks traffic. The effectiveness of the proposed system relies heavily on the willingness of ISPs in implementing the system. Once each ISP implements the system, most attacks can easily be stopped close to their point of origin. The main challenge is to implement such a system with the fixed amount of memory and available processing power with routers. A coordinated effort by participating ISPs filters out attacks close to their source, reducing the load on other routers. The suspicious traffic is first filtered out based on their source IP address. The authors also implemented the WRED algorithm for their case and conduct GNS3 experiments in a simulated environment.

INTRODUCTION

Denial of Service Attacks[1] aimed at various targets which led to the production of new challenges in the Internet within the network security communities and Internet Service Provider (ISP), to look for innovative and ingenious methods to secure our systems from these types of attacks. Denial of Service (DoS) attacks is mainly done in order to disrupt services. Hundreds or even thousands of compromised

DOI: 10.4018/978-1-7998-5348-0.ch011

hosts, called "zombies", are used to direct attacks to a particular host, in a Distributed Denial of Service (DDoS). These zombie hosts are usually unprotected computers connected to the internet through high bandwidth or always-on connection. Attackers recruit such hosts from millions of such computers by exploiting its vulnerabilities and planting sleeper codes that can quickly be activated with a command to launch DDoS attacks. The user or owner of such zombie hosts may not be aware that their system/ computer is participating in such activities. By overloading servers, DDoS attacks incapacitate network links, internet systems and connected devices with malicious or bogus traffic, unlike other attacks that are focused on stealing information penetrating security perimeters. With the growing dependence on internet, the impact of successful DDoS attacks on important installations can be devastating. Many websites have fallen victim to DoS attacks resulting in inconvenience and millions of dollars in damage[2]. The DDoS attacks have also caused a less severe but measurable consequences for the Composite Block List (CBL) as well as Project Honey Pot.

Many approaches and techniques have been proposed in the past years that help to prevent DDoS attacks (Kumar & Kumar, 2016; Shrivastava, Sharma & Rai, 2010; Sharma & Gupta, 2018). A structural approach to the DDoS problem was presented by developing a classification of DDoS attacks and DDoS defense mechanisms which placed some order in the existing approaches and defense mechanisms (Douligeris & Mitrokotsa, 2004; Rajkumar, 2013; Arora & Yadav, in press a; Arora & Yadav, in press b). Other approaches to prevent the DDoS attack that were proposed include techniques like web referrals (Desai, Patel, Somaiya & Vishwanathan, 2016) and linear prediction model (Gupta et al., 2010; Ahuja & Yadav, 2012, Al-Anzi, Yadav & Soni, 2014). In one approach multivariate data analysis was used to measure low and high rate DDoS attack (Hoque, Bhattacharyya & Kalita, 2016; Arora, Yadav & Sharma, 2018; Bhushan, Banerjea & Yadav, 2014; Dhingra & Yadav, 2017). In his paper, a DDoS mitigation system is proposed which uses access list-based configurations. These are deployed at the Internet Service Provider's (ISP) edge routers to prohibit DDoS attacks into and from the ISPs' networks. The effectiveness of the proposed system will rely heavily on the willingness of the ISPs in implementing the system. The following section discusses the problem identification and further the approach and mechanism of the proposed work and the implementation on the test environment are discussed.

TYPES OF ATTACKS

In this section, the two categories of DDoS attacks are explained in addition to DDoS attack taxonomy and well-known attacks.

Bandwidth Attacks

When a large amount of traffic is sent to the host or target network, an attack is carried out. This attack causes overuse of network bandwidth, memory or processing resources. If such traffic is left uncontrolled, devices in the target path such as routers, servers and firewalls can fail. In packet-flooding attack (a type of bandwidth attack) a large number of seemingly legitimate - UDP (User Datagram Protocol) or TCP (Transmission Control Protocol), ICMP (Internet Control Message Protocol) - packets are sent to a specific destination. These packets may misrepresent their source IP (Internet Protocol) address to make detection even more difficult and lead to "spoofing". An approach MULTOPS (MUlti-Level Tree for Online Packet Statistics) was proposed for bandwidth attack detection (Gil & Poletto, 2001).