Chapter 15
Performance Evaluation of Web Server's Request Queue against AL-DDoS Attacks in NS-2

Manish Kumar
Punjabi University, Department of Computer Engineering, Patiala, India

Abhinav Bhandari
Punjabi University, Department of Computer Engineering, Patiala, India

ABSTRACT

As the world is getting increasingly dependent on the Internet, the availability of web services has been a key concern for various organizations. Application Layer DDoS (AL-DDoS) attacks may hamper the availability of web services to the legitimate users by flooding the request queue of the web server. Hence, it is pertinent to focus fundamentally on studying the queue scheduling policies of web server against the HTTP request flooding attack which has been the base of this research work. In this paper, the various types of AL-DDoS attacks launched by exploiting the HTTP protocol have been reviewed. The key aim is to compare the requests queue scheduling policies of web server against HTTP request flooding attack using NS2 simulator. Various simulation scenarios have been presented for comparison, and it has been established that queue scheduling policy can be a significant role player in tolerating the AL-DDoS attacks.

INTRODUCTION

In today's digital era, the Internet has become the most common and widely used means of communication. Online services such as banking, shopping, gaming, social media and cloud storage are growing rapidly. Thus, its usage has been increased exponentially (INTERNET USAGE STATISTICS, 2015). The users communicate with each other through digital devices that interact via various protocols like ICMP, TCP, UDP, FTP, HTTP, and SMTP. Vulnerabilities in the protocols help the attackers to launch the attacks that may lead to severe loss especially in the financial sector. Few examples of attack types

DOI: 10.4018/978-1-7998-5348-0.ch015

are wiretapping, port scanning, the man in the middle, Denial of Service (DoS), E-Mail spamming and phishing. Among these attacks, DoS attack is the most critical one as its strength has increased much in the last few years (Worldwide Infrastructure Security Report, Volume XI, 2016). DoS attacks deny the services provided by the network or the servers to the legitimate users by overwhelming the resources. The attackers overload the resources by employing thousands of compromised machines into the attacks from all over the world; therefore, called Distributed Denial of Service (DDoS) attacks (McDowell, 2009).

Over the years, DDoS attackers have developed more strategic techniques to achieve their targets. They are now becoming more sophisticated since they are perpetrating the DDoS attacks of furtive nature that may prove to be very harmful. The attackers are now moving towards the stealthier DDoS attacks i.e. Application Layer Distributed Denial of Service (AL-DDoS) attacks. These attacks without causing any harm at the network layer and the transport layer reach the application layer (Durcekova, Schwartz, & Shahmehri, 2012). Consequently, the attackers are now posing a huge threat to the Internet Community and a significant challenge for the defenders of DDoS attacks.

From the past DDoS attack incidents on prominent organizations like Yahoo, eBay, Facebook, Twitter, US Banks and many others (Sachdeva, Singh, Kumar, & Singh, 2010; Zeb, Baig, & Asif, 2015; Mosharraf, 2015), it is noticeable that even a little unavailability of the web services can cause huge damage. By mimicking the behavior of legitimate users, AL-DDoS attacks have made this problem even more severe. So, to maintain the high availability of web services to legitimate users, during AL-DDoS attacks, is a major challenge. In this paper, the authors have evaluated the performance of web server's request queue policies so that the availability of web services can be sustained by tolerating the AL-DDoS attacks. The key contributions of the paper are:

- To review various types of HTTP based AL-DDoS attacks with an aim to get insight into the problem of AL-DDoS attacks;
- To launch the HTTP request flooding AL-DDoS attack by modifying the WebTraf module available in NS-2 Simulator;
- To evaluate and compare the performance of web server's request queue scheduling policies during HTTP request flooding attacks using relevant performance metrics like successful transactions, failed transactions, response time and server throughput.

RELATED WORK

By defending against DDoS attacks only through detection and traceback techniques does not completely solve the ever-growing problem of these attacks. The reason behind is to discriminate the attack packets from that of legitimate clients has become even more challenging due to legitimate mimicking behavior of AL-DDoS attacks. Moreover, the mimicking behavior of AL-DDoS attacks also increases the false positive and negative rates. However, the tolerance and impact analysis of DDoS attacks are also crucial to counter against these dreadful attacks. In 2003, (Xu & Lee, 2003) proposed a defense system that can sustain high availability of web services during the DDoS attacks. For this, the authors have segregated the legitimate traffic from the DDoS attack traffic by using a HTTP redirect message. They had measured the performance of this system by game theoretical framework. In (Farhat, 2006), the author proposed an implicit token scheme (ITS) so that the TCP services can be protected from DoS attacks. The researchers in (Beitollahi & Deconinck, 2009) conducted an empirical study to tolerate