Chapter 2
Denial-of-Service and Botnet Analysis, Detection, and Mitigation

Sobana Sikkanan
https://orcid.org/0000-0001-8237-7140
Adithya Institute of Technology, India

Kasthuri M.
PSNA College of Engineering and Technology, India

ABSTRACT

The internet is designed for processing and forwarding of any packet in a best effort manner. The packets carried by the internet may be malicious or not. Most of the time, internet architecture provides an unregulated path to victims. Denial-of-service (DoS) attack is the most common critical threat that causes devastating effects on the internet. The Botnet-based DoS attack aims to exhaust both the target resources and network bandwidth, thereby making the network resources unavailable for its valid users. The resources are utilized by either injecting a computer virus or flooding the network with useless traffic. This chapter provides a systematic analysis of the causes of DoS attacks, including motivations and history, analysis of different attacks, detection and protection techniques, various mitigation techniques, the limitations and challenges of DoS research areas. Finally, this chapter discusses some important research directions which will need more attention in the near future to guarantee the successful defense against DoS attacks.

INTRODUCTION

In the modern era, our daily life depends on Internet applications for all our necessary activities. Some humans are using this internet in a destructive manner and some others use this in a constructive manner. Cloud computing has an impact on the growth of internet word even though the process of designing and computing of a cloud environment is complicated (Kumar, 2018). The complexity of the cloud-computing

DOI: 10.4018/978-1-7998-5348-0.ch002

process leads to insecure digital data processing (Feng, Chen, & Liu, 2010). A collection of hijacked devices connected through the internet represents a Botnet which creates some safety and security issues. Bailey, Cooke, Xu, and Karir (2009) stated that the detection and mitigation of these botnet threads is a complicated process. Botnet cyber-attacks such as Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks are introduced to steal a victim's personal information (Aamir & Zaidi, 2013).

Initially, the DoS attacks were introduced against web applications. The first DoS attack was initiated by the hijackers in the late 1990s and it becomes a significant danger to all the web applications (Bencsáth & Vajda, 2004). As said by (Gresty, Shi, & Merabti, 2001), DoS controls the web pages for a predefined amount of time to collect all the personal information and introduces some revenue lost even in the offline condition. In business environments, companies try to knock off their competing companies from the business market with the help of these DoS attacks. Pappalardo (2005) revealed that online extortion via DoS attacks is increasing during the past decades. Attackers controlled the victim's online businesses using DoS attacks and threatened them to give payments for their protection.

In recent network scenarios, most of the companies, organizations, and government sectors are looking forward to transferring all or parts of their information to the cloud (Gonzales D, Kaplan J.M, Saltzman E, Winkelman Z, & D., 2017; Wong, 1998). The introduction of cloud technology allows the organization to transfer a lot of information with the least capital cost. DoS aims to attack widely used public sectors such as Banking services and e-commerce sites. DoS attack introduces some massive security threats to some government organizations such as India in 2012 (Register., 2012), the USA in 2015 (Incapsula., 2015), Brazil in 2016 (Corero., 2016) and Ireland in 2017 (Silicon., 2017). DoS attackers used some malware techniques to hack the details of customers of U.S based banks in 2012 (Networks, 2012). HSBC bank in the U.K was in the hit list of DoS attack during 2016 (Guardian., 2016). E-commerce sectors such as Bitcoin websites were also affected by DoS attacks in 2017 (Coindesk., 2017). Recent years DoS causes a significant impact on social websites like eBay, Amazon, Buy.com, Capital one bank, SunTrust bank, and Microsoft. The above discussions reveal that protecting the network from the DoS attack becomes an important issue (Arunadevi, 2018). The inability of the network security mechanism in detecting the DoS attack indicates the lack of security services in the government structure.

A lot of DoS detection and prevention techniques were introduced in the past decades (Jayanthi, DileepKumar, & Singh, 2016; Sharma & Gupta, 2018; Shrivastava, Sharma, & Rai, 2010). But still, DoS remains a significant challenge to network security systems because of its implementation complexity (Amit & Santhithilagam, 2019). Different types of DoS attacks and the different defense mechanism involved in detection and prevention process leads to the development of a structural approach to the DoS defense mechanisms (Arushi Arora, Sumit Kumar Yadav, & Sharma, 2018; Douligeris & Mitrokotsa, 2004). Linear predictor model (Al-Anzi, Yadav, & Soni, 2014; Gupta et al., 2010),web referrals (Desai, Patel, Somaiya, & Vishwanathan, 2016) and multivariate data analysis to measure the low and high rate DDoS attack (Arushi Arora et al., 2018; Bhushan, Banerjea, & Yadav, 2014; Hoque, 2016) are some of the existing approaches to prevent proposed the DDoS attack. In 2018 Yadav, Sharma, and Arora (2018) proposed a list-based DDoS mitigation system configurations. This mitigation software are developed by the edge router of the Internet Service Provider (ISP) to rule out DDoS attacks into and from the ISPs' networks.

This chapter discusses in detail about the causes of DoS and DDoS, different types of DoS attacks, the motivation of different DoS attacks, available protection, and mitigation techniques and the challenges associated with modern techniques. The chapter also gives some research directions to overcome the DoS and DDoS security attacks. This chapter is organized as a combination of seven subdivisions.