Computers and Electrical Engineering 72 (2018) 26–38

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Defense mechanisms against Distributed Denial of Service attacks : A survey☆

Mousa Taghizadeh Manavi

Young Researchers and Elite Club, Ardabil Branch, Islamic Azad University, Ardabil, Iran

ARTICLE INFO

Article history:
Received 1 November 2016
Revised 4 September 2018
Accepted 4 September 2018

Keywords:
DDoS attack
Bot
Source-based
Network-based
Destination-based
Hybrid mechanism

ABSTRACT

Distributed Denial of Service (DDoS) attacks are a group of collaborative attacks performed by attackers threatening internet security and violating services. In this attack, the attacker makes use of compromised systems to prevent legitimate users from having access to the server resources and use them to provide extensive attacks against the victim. In this paper, we surveyed defense mechanisms against DDoS attacks which are useful in internet. We categorized the mechanisms into two layer-based main groups of network/transport layer and application layer. Then, the network/transport layer is classified into four classes of source-based, network-based, destination-based and hybrid mechanisms, and the application layer mechanisms are categorized into two classes of destination-based and hybrid mechanisms. We surveyed important developments in each of the aforementioned classes and outlined new challenges. This survey paper provides a discussion of the difference between the aforementioned mechanisms categorizations based on characteristics of the way of detection, defense, and response as well as orientations for future researches.

1. Introduction

Nowadays, the ever increasing growth of internet has become a factor of evolution in human life and it has been known as an effective, unavoidable technology to meet human life demands. The internet has its advantages and disadvantages like other available facilities. Advantages of internet include scalability and easy communication. In contrast, one of the main challenges of this technology is security, which has experienced numerous variations through time. Denial of Service (DoS) attack is a dangerous threat in the internet. In DoS attack, the attacker invades the intended victim (server) and makes the services offered to legitimate users unavailable. Consequently, DoS attack may be considered as a threat for internet availability [1]. By the advent of DoS attacks, different websites and servers such as Yahoo, eBay, and Amazon has been invaded by this kind of attack, which imposed huge financial losses to the companies and their servers. Since there was an attacker in DoS attack, it was not possible to perform heavy, extensive attacks and the attacker was identified easily. By the growth of internet in the last decade, however, the attackers' function has developed and unfortunately, the system's vulnerability in terms of security has increased; vulnerable systems have paved the way for attackers to perform massive attacks. Using this kind of attack is known as DDoS attack. This kind of attack, which acts cooperatively and is performed in large scale, is performed directly by compromised computers. An example of DDoS attack general architecture is shown in Fig. 1. In DDoS attack, there are two types of victims regarding the exploitation of compromised computers

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Area Editor Dr. G. Martinez

E-mail address: mosatagi98@yahoo.com

https://doi.org/10.1016/j.compeleceng.2018.09.001
0045-7906/

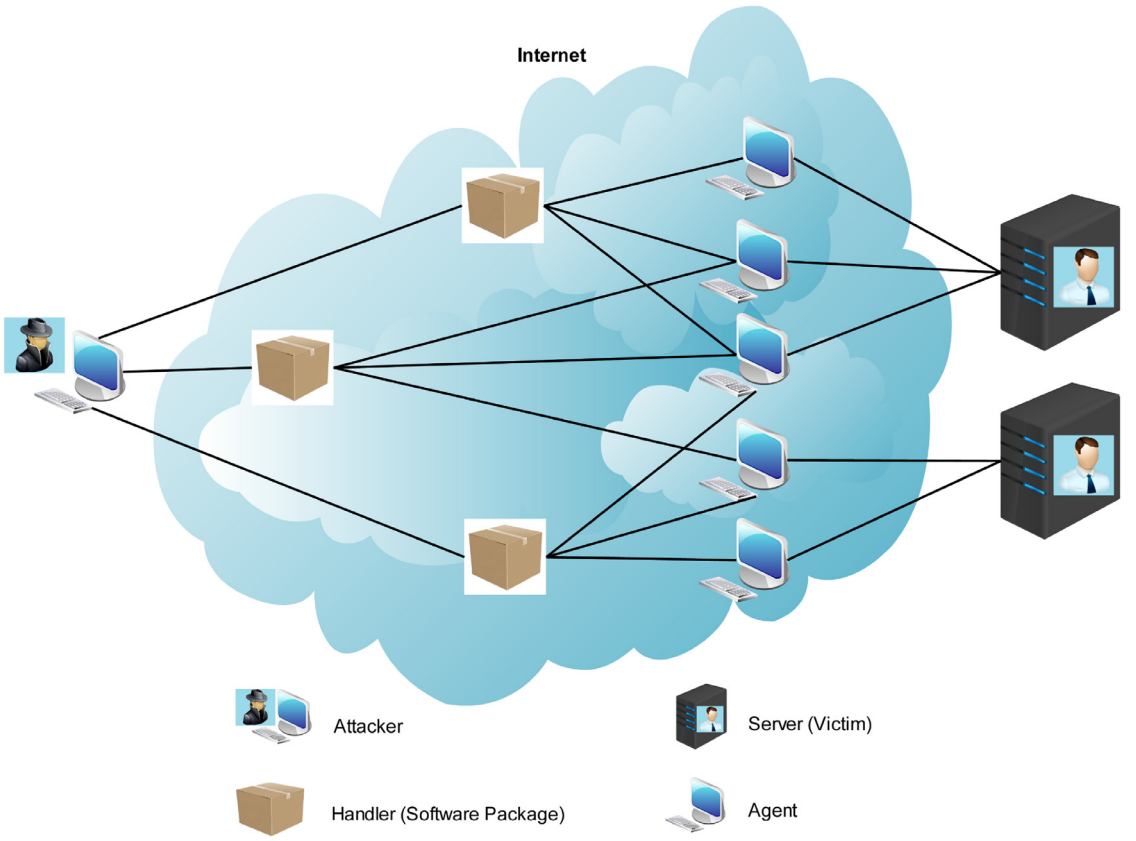

Fig. 1. The general architecture of DDoS attack.

by the attacker. The first victim type is the server, or in other words, it is the main target of the attacker and the attacker can exhaust its computational resources or make the victim's communication link unavailable by flooding. The second type of victims includes vulnerable systems which are controlled by the attacker. Accordingly, first, the attacker compromises a large number of internet hosts by installing the software, and then installs the attack software on the compromised systems. These compromised systems are known as bots or agents, which are controlled by the attacker using handler systems. Such a network which is controlled by the attacker is called Botnet or Zombies network. In the next step, the attacker sends commands to the bots using handlers and bots invade the server by generating high volume packets. As a result, the server is not able to respond to a high volume of packets and its resources exhaust quickly.

Nowadays, due to the progress made in DDoS attacks and new complex, destructive tools designed by attackers, novel defense mechanisms and methods have been proposed by the researchers, which are categorized in specific groups based on their application, location, and defense type. One popular categorization for defense mechanisms is based on the location of detection and defense against attack. Consequently, the proposed methods may be categorized into source-based, network-based (core), destination-based, and hybrid groups; this kind of categorization is referred to and used in [2]. Due to the extensive methods used in detecting DDoS attack and defending against them, different kinds of classifications in network/transport and application layers have been proposed in [3]. In this paper, we mostly divided the introduced mechanisms for DDoS attacks detection and defense into two main groups (Fig. 2) of network/transport layer and application layer, based on [2] classification. Due to different circumstances of layers in the network, defense mechanisms' classification based on layers and protocol types separates each method properly based on the function and operational domain. In this paper, network/transport layer mechanisms are divided into four groups of source-based, network-based (core), destination-based, and hybrid (distributed) mechanisms, and the application layer is divided into two groups of destination-based (server side) and hybrid mechanisms (distributed). A number of review papers in the context of DDoS attacks and mechanisms have been presented before; but this review paper is different from previous papers in many aspects: (1) Basic DDoS attacks are introduced and described, since new attacks are based on basic attacks. (2) There are different categories of defense mechanisms where each category has its own advantages and disadvantages; since defense mechanisms are specified based on network or application nature, and also considering defense type, determining location and region of implementing mechanism significantly affects defense. Thus, in this paper, mechanisms are classified based on being network/transport or application, and defense location. (3) In classifying mechanisms based on location, defense location is specified based on