Journal of Network and Computer Applications 58 (2015) 165–179

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Review

Taxonomy of Distributed Denial of Service mitigation approaches for cloud computing

Alireza Shameli-Sendi [a,*], Makan Pourzandi [b], Mohamed Fekih-Ahmed [c], Mohamed Cheriet [c]

[a] School of Computer Science, McGill University, Montreal, Canada
[b] Ericsson Security Research, Ericsson, Montreal, Canada
[c] Synchromedia Lab, Ecole de Technologie Superieure (ETS), University of Quebec, Montreal, Canada

ARTICLE INFO

Article history:
Received 23 May 2015
Received in revised form
17 July 2015
Accepted 29 September 2015
Available online 9 October 2015

Keywords:
Distributed Denial of Service (DDoS)
DDoS detection
DDoS mitigation
Defense system
Cloud computing
Software-Defined Networking (SDN)

ABSTRACT

Cloud computing has a central role to play in meeting today's business requirements. However, Distributed Denial-of-Service (DDoS) attacks can threaten the availability of cloud functionalities. In recent years, many effort has been expended to detect the various DDoS attack types. In this survey paper, our concentration is on how to mitigate these attacks. We believe that cloud computing technology can substantially change the way we respond to a DDoS attack, based on a number of new characteristics, which were introduced with the advent of this technology. We first present a new taxonomy of DDoS mitigation strategies to organize the work. Then, we go on to discuss the main features of existing DDoS mitigation strategies and explain their functionalities in the cloud environment. Afterwards, we show how the existing DDoS mechanisms fit into the network topology of the cloud. Finally, we discuss some of these DDoS mechanisms in detail, and compare their behavior in the cloud. Our objective is to show how these characteristics bring a novel perspective to existing DDoS mechanisms, and so give researchers new insights into how to mitigate DDoS attacks in the cloud computing.

Contents

* Corresponding author.
E-mail addresses: alireza.shameli-sendi@cs.mcgill.ca (A. Shameli-Sendi), makan.pourzandi@ericsson.com (M. Pourzandi), mohamed.fekih.ahmed@synchromedia.ca (M. Fekih-Ahmed), mohamed.cheriet@etsmtl.ca (M. Cheriet).

http://dx.doi.org/10.1016/j.jnca.2015.09.005
1084-8045/

1. Introduction

Cloud computing has a central role to play in meeting today's business requirements. Following the lead of early cloud providers (Amazon, Google, IBM, etc.), organizations such as banks, corporations, hospitals, and medical centers have begun to rely on cloud services. However, DDoS attacks can be a major threat to the availability of these services (Zissis and Lekkas, 2012; Subashini and Kavitha, 2011; Bhadauria et al., 2011; Zhang et al., 2012). According to the Cooperative Association for Internet Data Analysis (CAIDA), over 5000 DDoS attacks occur on the Internet every week (Zargar et al., 2013).

DDoS attacks, as the name implies, involve a large number of distributed hosts generating traffic that is directed at a selected target (Huici and Handley, 2007). Attack vectors can be categorized into two groups (Ranjan et al., 2009; Walfish et al., 2010; Spyridopoulos et al., 2013), brute-force and semantic. Brute-force attacks, also known as "flooding attacks", focus on bandwidth consumption by invoking vast numbers of bogus requests, aggregating the traffic of a large number of distributed hosts, and overwhelming the target (Argyraki and Cheriton, 2009). These targets can be applications, hosts, or infrastructure. An example of a brute-force application attack would be a large number of SSH login attempts on all elements of a provider's network (McPherson, 2010). A brute-force attack, because of its distributed nature, can be massive. The biggest botnets currently hold over a million bots, and estimates of the number of bots involved in any particular DDoS range from a few thousand to upwards of 10,000 (NetworkWorld, 2009).

In contrast, semantic attacks, also known as "vulnerability attacks", focus on resource starvation by exploiting protocol weaknesses (Mirkovic and Reiher, 2004). The latest trend is to carry out an application-level attack, based on HTTP, HTTPS, or DNS, for example. This type of attack does not cause major congestion, but it is harder to detect and so more challenging to fight. A semantic attack attempts to exploit a weakness, rather than exhausting bandwidth/resources, and generally targets a protocol or an application. A DDoS on a protocol does not necessarily involve the characteristic of flooding by massive amounts of traffic. A well-known example would be the TCP SYN attack, which exploits the allocation of a connection context in the server (Moore et al., 2006; Argyraki and Cheriton, 2009).

As Fig. 1 illustrates, the DDoS defense life-cycle consists of four phases: *prevention*, *monitoring*, *detection*, and *mitigation*. In the prevention phase, appropriate security appliances are put in place at different locations to secure services and data against DDoS attack. In the monitoring phase, tools are deployed to gather useful host or network information to follow the execution of the system. The detection phase involves analysis of the systems that are running, in order to find the source of malicious traffic or malicious attempts to cause DDoS (Abliz, 2011; Shin et al., 2013). The final phase, mitigation, completes the defense life-cycle by evaluating the severity of the attack and selecting the right response (Shameli-Sendi and Dagenais, 2013) at the right time (Shameli-Sendi et al., 2012). In the mitigation phase, a response system selects appropriate countermeasures to effectively handle a DDoS attack or slow down the malicious clients (Walfish et al., 2010).

Existing defense mechanisms against DDoS attacks have limited success because they cannot meet the considerable challenge of achieving simultaneously efficient detection, effective response, acceptable rate of false alarms, and the real-time transfer of all packets (Zargar et al., 2013; PC World, 2013). Prevention and poor detection alone have resulted in huge financial losses to leading businesses around the world (Alomari et al., 2012). Strategies and heuristics for DDoS detection have been researched extensively (Yu et al., 2009). In real world, it is not possible to detect attacks with 100% accuracy (Yu et al., 2012). Therefore, there is a need to concentrate on more efficient mitigation mechanisms. The cloud by its very nature is more exposed to DDoS attack, but it also provides us with additional means to protect applications against DDoS attacks. Therefore, in this work, we mean by DDoS detection the implementation of mechanisms designed to identify the source of malicious traffic or malicious flows, and we define DDoS mitigation as the implementation of mechanisms designed to eliminate the malicious traffic.

Several taxonomies of DDoS defense techniques have been proposed in the literature (Zargar et al., 2013; Geng et al., 2002; Wood and Stankovic, 2004; Mirkovic and Reiher, 2004; Peng et al., 2007; Abliz, 2011). Mirkovic and Reiher (2004) and Zargar et al. (2013)) propose taxonomies for classifying DDoS attacks and defense techniques, while Peng et al. (2007) propose a taxonomy

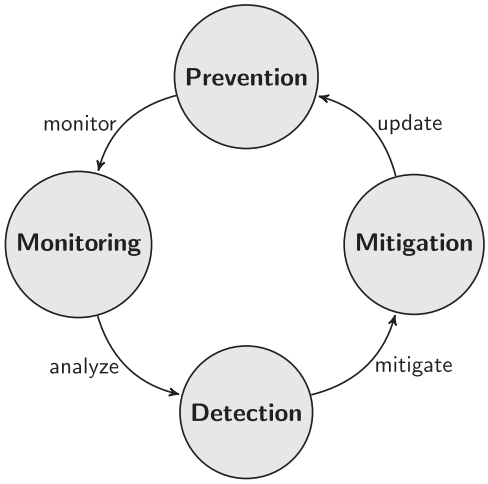

Fig. 1. Defense life-cycle.