Computers and Electrical Engineering 000 (2016) 1–15

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

DDoS victim service containment to minimize the internal collateral damages in cloud computing☆

Gaurav Somani[a,b,*], Manoj Singh Gaur[b], Dheeraj Sanghi[c], Mauro Conti[d], Muttukrishnan Rajarajan[e]

[a] Central University of Rajasthan, Ajmer, India
[b] Malaviya National Institute of Technology, Jaipur, India
[c] Indian Institute of Technology, Kanpur, India
[d] University of Padua, Padua, Italy
[e] City University of London, London, UK

ARTICLE INFO

Article history:
Received 30 April 2016
Revised 5 December 2016
Accepted 5 December 2016
Available online xxx

Keywords:
Cloud computing
Cloud security
Distributed Denial of Service (DDoS) attack and Economic Denial of Sustainability (EDoS) attack

ABSTRACT

Recent Distributed Denial of Service (DDoS) attacks on cloud services demonstrate new attack effects, including collateral and economic losses. In this work, we show that DDoS mitigation methods may not provide the expected timely mitigation due to the heavy resource outage created by the attacks. We observe an important Operating System (OS) level "internal collateral damage", in which the other critical services are also affected. We formulate the DDoS mitigation problem as an OS level resource management problem. We argue that providing extra resources to the victim's server is only helpful if we can ensure the availability of other services. To achieve these goals, we propose a novel resource containment approach to enforce the victim's resource limits. Our real-time experimental evaluations show that the proposed approach results in reduction in the attack reporting time and victim service downtime by providing isolated and timely resources to ensure availability of other critical services.

1. Introduction

Distributed Denial of Service (DDoS) attacks result in fatal attack effects to enterprises for last many years. DDoS attacks are also visible by service downtimes faced by important services, and remain among the top cyber security threats for the last several years. There are reports which state that one out of five enterprises across the world is affected by DDoS attacks [1]. The growth of DDoS attacks can be visualized by the progress of these attacks made from the perspective of maximum attack bandwidth each year. The peak DDoS attack bandwidth reached more than 500 Gbps in 2015 from just 8 Gbps in year 2000 [2]. Major motivation behind DDoS attacks includes business rivalry, political ideology, and cyber war among countries. The most common outcome of DDoS attacks is "unavailability of target service". In addition to the unavailability, there are many short term and long term business and reputation losses, which are actually a set of consequences of the service downtime.

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

* Corresponding author.
E-mail address: gaurav@curaj.ac.in (G. Somani).

http://dx.doi.org/10.1016/j.compeleceng.2016.12.004
0045-7906/

In recent times, cloud computing has been adopted across the globe to support the major IT requirements of organizations from all industry sectors. As highlighted in [3], majority of the organizations (>87%) across the globe are using cloud infrastructure to run their mission-critical applications. This adoption trend is due to the profound resources and availability of on-demand resources in the cloud. However, the emergence of cloud computing has also led to the shift of DDoS attackers more towards the cloud driven services. As highlighted in [2], more than 33% of the overall reported attacks in year, 2015 were targeted towards cloud services. In addition, cloud features such as profound resources and pay-as you go accounting are also becoming attractive to the attackers.

The DDoS attacks in cloud computing are also termed as Economic Denial of Sustainability (EDoS) attacks, due to the substantial economic losses both from resource usage and business disruption. These losses are directly proportional to the downtime incurred by the attack. Most of the reported attacks usually last between few minutes to few hours [2] and some "major" attacks may last few days to even weeks. There are many recent DDoS attacks on cloud services among which the attacks on Amazon EC2 services, RackSpace and Linode are major incidents resulting into considerable service outages.

There are a large number of DDoS mitigation solutions available today, which are summarized in recent survey articles [4] for traditional fixed and cloud infrastructures [5]. On the other hand, there are solutions used by service providers, which mostly work on traffic filtering and quick attack absorption by resource scaling [6]. The cost factor is one of the major features to attract the service providers to migrate to the cloud infrastructures. The cost to eliminate the DDoS attack effects is an important aspect to consider during mitigation, as it directly comes from the economic sustainability of the victim's enterprise. There are also recent DDoS attack incidents, where the "Service Denial" does not seem to be the main focus of the attackers. These hidden attacks usually launch a DDoS attack in order to achieve the whole attention of the victim and simultaneously perform other severe activities such as data breaches. These attacks are termed as "Smoke-screening attacks" [7]. These attack effects are possible due to the heavy resource investment (both in terms of manpower, server and network resources) in DDoS mitigation leaving other important activities unattended.

Similarly, multi-tenancy, auto scaling and migration of services lead to some additional effects of DDoS attacks in cloud computing. These attacks are termed as "collateral damages" on co-hosted cloud services and network components [8]. The above discussion makes it necessary for availability of efficient solutions in the direction of DDoS attack prevention, detection and mitigation. DDoS attacks are usually considered resource intensive requests, which stress overload one or a combination of target service resources. These resources are usually the basic resources like CPU cycles, memory and swap usage, I/O operations or network bandwidth. Additional application level resources are number of simultaneous connections, ports, sessions, application buffers or other temporary identifiers. Most of the server resources are shared among many of the co-located processes to achieve their goals. Victim service, DDoS mitigation service, logging and scheduling processes are few examples of such processes.

In this work, we provide a novel observation towards operating system level resource race and contention among co-located services. We argue that the services co-located with the DDoS victim service (say a web-server process) may not provide the expected processing and timely outcome due to the extensive resource contention by the DDoS attack. These co-located services include all the important services, such as DDoS mitigation service, firewall and internal security policy services (e.g. SELinux) to other system processes and remote login processes. We show this phenomenon in the experiments and term it as "Internal Collateral Damage" as the services other than the victim service, is severely affected. We show that DDoS Mitigation methods may not provide the expected outcome and delivery due to this factor. To approach the "internal collateral damage" problem, we provide an analysis of DDoS attacks from the OS level resource management perspective. Usually, virtual machines (VMs) are used across clouds to provide strong performance and resource isolation. However, the internal operating system level isolation cannot be governed by the virtual machines.

We argue that resource isolation among co-located services, may provide quick and efficient DDoS mitigation. Based on these requirements, we propose a novel approach, "Victim Service Containment" to achieve resource contention of victim service resources which is under attack. We perform real-time attack experiments to show that the proposed approach provides resources availability to all the important services and help to minimize the overall attack effect and cost. We provide attack cases and model resource requirements to provide solutions based on resource control groups [9] to provide internal isolation without affecting the performance. We also extend the discussion to limit DDoS effects to just the target service, to eliminate or minimize additional collateral damages.

The rest of the paper is organized as follows. Section 2 provides the details about DDoS attack protection at various levels of the cloud architecture. Section 3 provides details of the experiments showing the novel "Internal Collateral Damages". We provide a detailed resource management model of the problem in Section 4. Section 5 provides the proposed design to eliminate the internal collateral damages. Section 6 provides the details of the evaluation to show the efficacy of the proposed solution. We also discuss the features of the proposed solution and various aspects related to DDoS mitigation. We provide a discussion of the related work in Section 7 and finally conclusions in Section 8.

2. DDoS attack and protection in the cloud

DDoS attacks are mostly coordinated attacks planned by a command and control (C & C) server with the help of a malware infected network of computers. These computers are also known as "bots". Cloud infrastructure can also be used in the networks of attack computers with the emergence of pay-as-you-go "DDoS for hire" services. The impact of these attacks depend upon various attack dimensions.

Please cite this article as: G. Somani et al., DDoS victim service containment to minimize the internal collateral damages in cloud computing, Computers and Electrical Engineering (2016), http://dx.doi.org/10.1016/j.compeleceng.2016.12.004