Chapter 25
DOS Attacks on Cloud Platform: Their Solutions and Implications

Rohit Kumar
Chandigarh University, India

ABSTRACT

IaaS, PaaS, and SaaS models collectively form the Cloud Computing Infrastructure. The complexity of interrelationship of service models is very high and so security issue becomes essentials and must be developed with utmost care. Distributed DOS attacks are a major concern for different organization engaged in using cloud based services. The denial of service attack and distributed denial of service attacks in particular in cloud paradigms are big threat on a cloud network or platform. These attacks operate by rendering the server and network useless by sending unnecessary service and resource requests. The victims host or network isn't aware of such attacks and keeps providing recourses until they get exhausted. Due to resource exhaustions, the resources requests of genuine users doesn't get fulfilled. Severity of these attacks can lead to huge financial losses if, they are able to bring down servers executing financial services. This chapter presents DOS threats and methods to mitigate them in varied dimensions.

INTRODUCTION

Cloud computing has gained significant importance and has become obvious part of our day to day computation and communication needs. The cloud provides a platform for computation in terms of both hardware and software. The IaaS, PaaS and SaaS are cloud based services and provide online storage spaces, computational platform, customized software's etc. With more and more dependence on cloud computing, the issue of security becomes very important and is critical to the success of cloud based services. Many type of threats exists in cloud domain but, in this chapter we particularly focuses on Denial of Service attacks and methods to control them.

Denial of service attacks (DoS) are well known attacks and poses a serious problem in internet and other types of networks. The goal of DoS is to disturb the services and making them inaccessible to the user. In this kind of attack the network is rendered useless by attacking vehemently on the bandwidth and

DOI: 10.4018/978-1-7998-5348-0.ch025

connectivity. In these attacks the attacker sends a large stream of packets which causes huge congestion on the victims network. Due to this high congestion, the network cease to works and even a single request doesn't get served. In past there have been numerous attacks of these kind which targeted many famous internet sites and exposed their vulnerabilities. The distributed DOS called DDOS has been a complex and powerful technique to attack internet and its resources. As multiple machine or attackers can target a single machine; to identifying the real attackers for such attacks and to mitigate their effect is very difficult to achieve. The internet protocols like TCP/IP are well studied and some of them provides open resources access model which makes them easily targetable by the attackers. The attackers targets the some key loopholes in the internet system architecture to carry out such attacks. The DDOS attacks are called many to one attack as multiple sources attacks a single machine in well planned and synchronized way. These multiple attacker machines strangulates the target machine by huge data i.e. large volume of data or packet steams are sent to target machine to swamp it and efforts are made to make these packets genuine, this process renders the target useless. The traffic or data from multiple machines is transferred in aggregated and intelligent manner so that the target cannot distinguish among them and treat them as genuine and valid packets. The attacker usually knows the traffic handling capacity of the target and generates far more data than its capacity. The DDOS attack can damage the target form moderate to critical level. These attacks can lead the system to get shutdown, to corrupt files and usually results in total or partial loss of services.

The difficult thing about DDOS is that there is no clearly apparent feature which can lead to detection of these attacks. So, clear and direct methods to deal which such attacks aren't easy to devise and implement. The attackers now a days has access to user friendly and easy to use software's which assists in carrying out these attacks and averagely secured machine cannot handle such attacks.

The DoS attacking programs are devised with simple logic and occupy small memory making their handing easier. The attackers are vigilant and keep on devising new methods to carry out such attacks and its reverse is reciprocated by the defenders. The defenders must be pro-actively vigilant to secure their system. The DDOS handling technique are growing at a rapid rate but, a real panacea for such attacks is difficult to achieve. In practice multiple flavours of these attacks exists and providing a safe solution for all of them is very difficult to achieve. The mitigating techniques employed for such attacks tries to stop the attacker by making such attack difficult to carry out and making the attacker accountable for these attacks.

CLASSIFICATION OF DOS ATTACKS:

The DoS attacks can be carried out in different ways. The major distinguishing features has been mentioned here. Figure 1 presents the classification of DoS attacks. Below is a brief introduction to these attacks:

- **Network Device Level Attack:** DoS attacks in network device level can be caused by exhausting hardware resources of network devices (Douligeris, 2004) and by exploiting bugs in software also. One of the most common examples of such attack is buffer overrun attack. Some password checking routines are not well coded and can easily become target of buffer overrun attack by entering long passwords.