Threat in Cloud- Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attack, and Security Measures

Khalid H Alotaibi
Information Security, Lewis University
abomutaze@hotmail.com

ABSTRACT
Cloud computing is a technology which has witnessed spread after using widely the Internet, and the big brand companies has introduced this type of industry, which is a pioneer technology in delivering services over the Internet to more efficiently and lowest cost for enterprises. However, there are challenges that face this industry; one of these challenges is the Denial of Service (DoS) and Distributed Denial of Service (DDos) attacks. This paper is going to reach the effect of these attacks on the Cloud Computing. Furthermore, it is listed some different types of these attacks, their effects, and approaches to mitigate these attacks. It is also listed the important basic countermeasures, which help organizations to mitigate denial of service attacks. The most serious threats of the denial of service attacks to cloud computing are XML-based Denial Service (X-DoS) and HTTP-based Denial of Service (H-DoS) attack, which is difficult to stop them by basic countermeasures. This paper analysis how X-DoS/H-DoS attacks affect cloud computing, and mention some security solutions to prevent them.

Keywords: Threats in Cloud computing.

1. INTRODUCTION
Today, cloud computing has become the most important service in the internet, because it provides wide variety of services to users like store data. There are emerged challenges, which threaten this technology. According to the Cloud Security Alliance, reported that the Denial of Service was the fifth threat of top notorious nine in cloud computing in 2013. [7] A distributed denial of service (DDoS) attack and a denial of service (DoS) attack has become the main threat to the internet communication world, this is because they cause stopping of services, and may lead to damage in hardware or data. A DDoS attack defined as many hosts attacking one host in order to degrade its services or its complete removal from internet. These attacks deprive legitimate users to use the target’s services by depleting communication and resources of the victim. According to a study that was done by Ponemon Institute (November, 2012), indicates that 65% of surveyed organizations had attacked by an average of three DDoS attacks in the prior twelve months with an average annual cost of $3,000,000. It is becoming a mainstream. [6] In the area of cloud computing, these attacks have increased dangerous due to grow users and applications that connect with a cloud system. That leads the cloud system receives many requests. Also, the cloud server provider would lose a lot of money if its services were not available.

2. THE IMPACT OF DOS AND DDOS ATTACKS ON CLOUD COMPUTING
As most clouds are in commercial use now, so securing resources and the users is a prime priority, and maintaining integrity, confidentiality, and availability are the main goal to continue the business. The challenges that are faced a cloud sever provider (CSP) are that prevent the cloud from any serious attacks of effect on the performance of the cloud computing model. As a CSP depends on the Internet to provide its services; it may be able to ensure integrity, confidentiality. However, availability is the strong challenge which terrifies a CSP because it influences business continuity and productivity, and customer satisfaction. Denial of service attacks are campaigns to aim traffic and servers, that causes disruption of bandwidth or resources. This threatens clearly for availability security. A DoS and a DDoS attack might rarely affect confidentiality and integrity. This is because these attacks happen in short time for making network or a host is unavailable, however, they may increase potential risks. For example, when a server is attacked by a DoS or DDoS, this could be stopped some services of security against intrusion. Thus, the server will be compromised to be infected by malware or easy hacked.

3. TYPES OF DOS AND DDOS ATTACKS
Although the Denial of Service attacks are in general similar in consequence that is unavailability of service, they have different effects on a server and a network, and different attack mechanisms, and thus these attacks would need different defense approaches to mitigate them. Some different types of the Denial of Service attacks along with their impacts, and solutions are explained in the table given below:
Table 1: Some DoS & DDoS Attacks, and their effects on the cloud, and solution

<table>
<thead>
<tr>
<th>NO</th>
<th>Name of the attack</th>
<th>Effect of attack</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bandwidth Attack</td>
<td>Generating a traffic overload. Consequently, it cripples a victim's resources</td>
<td>Use MULTOPS (Multi-Level Tree for Online Packet Statistics), which is the tree of nodes for monitoring certain traffic characteristics in the network device like as a router. [8]</td>
</tr>
<tr>
<td>2</td>
<td>ICMP (Ping) Flood</td>
<td>Consumes victim's resources by many ICMP echo requests.</td>
<td>Configure the firewall by using ScreenOS, which sets a threshold that protects against the ICMP flood attack feature.[9]</td>
</tr>
<tr>
<td>3</td>
<td>Amplification attack</td>
<td>Attackers amplify the network traffic by making a request which generates a larger response.</td>
<td>Load balancer, limiting the connection and the connection rate, and should use OS that has high performance. [10]</td>
</tr>
<tr>
<td>4</td>
<td>DNS Flood</td>
<td>Assaults both DNS application and infrastructure.</td>
<td>Mitigating response time, which can use Radware that protects from DNS attacks. [10]</td>
</tr>
<tr>
<td>5</td>
<td>HTTP GET Flood</td>
<td>A server receives a huge request, which consumes its resources.</td>
<td>Configuring Firewall and Intrusion prevention system, and placing a device anti-DDOS. [10]</td>
</tr>
<tr>
<td>6</td>
<td>Reflector Attack, is known DRDoS (Distributed Reflection Denial of Service)</td>
<td>Attackers use the requested responses of routers and servers for reflecting attack and hiding their source, which causes consuming bandwidth.</td>
<td>Use DERM (Deterministic Edge Router Marking), which filters packets of the attack traffic, and identifies the source of the attack. [10]</td>
</tr>
</tbody>
</table>

4. COUNTERMEASURES AGAINST THE DOS AND DDOSS

In general, there are necessary measures should be implemented to contribute in securing an organization's systems against the most denial of service attacks. These measures are:

- Determine vulnerabilities in systems: this step is very important to stand on a system's ability to face risks of attacks. IT administrators have to scan their systems periodically to detect DoS vulnerabilities. They can use vulnerability scanning tools like as Qualys guard, Metasploit, or Nessus to determine vulnerabilities and weaknesses that can be exploited to launch a D/DoS attacks. After that, should implement security controls to fix the identified security issues. [1].
- Use Intrusion Detection tools: This defense mechanism can monitor networks for DoS attacks; it includes two methods of intrusion detection. The Behavior-based method which works to compare the usual behavior with the recent user actions. Another method is the Knowledge-based method which identifies known attacks. The odd behaviors would be analyzed by using artificial intelligence. Therefore, the IDS is very helpful to detect the attack traffic, alert the other nodes, and take corrective actions to prevent it. [1], [2].
- Update patches: there is a race between corporations, which issue software, and hackers who always seek to detect and exploit vulnerabilities in software. Hence, IT administrators have to update regularly security patches and software. Older versions of software and operating systems are usually vulnerable to security attacks, because attackers identified weaknesses and how to exploit. So, IT administrators should test regularly for security updates and install them on appliances like network hosts, routers, and firewalls. [1].
- Configure firewall rules: although the firewalls are an essential security measure to secure organizations, they are only not enough to prevent D/DoS attacks, because they were not designed to address DDoS threats. Firewalls work to determine which traffic should pass through into the network. This is based on predetermined rules. Thus, they cannot distinguish between malicious and legitimate users. However, the firewalls are as the first line of defense in the organization. Firewalls can filter three levels, the IP packet, the TCP session, and the application. That helps to monitor and filter out malicious traffic and IP address to prevent IP spoofing. [1][3]

These security measures that are mentioned above are countermeasures to safeguard from the most kinds of DoS and DDoS attacks. However, there are different types of these attacks, which target the cloud computing for exploiting its vulnerabilities. Sometimes, attackers during their campaigns to launch DoS and DDoS attacks by using complicated tools such as Mstream, Agobot, and Trinoo. But, most attackers have moved to use the less complex tools such as Extensible Markup Language (XML) based Denial of Service (X-DoS) and Hypertext Transfer Protocol (HTTP) based Denial of Service (H-DoS).This is because these tools are
implemented easily attacks. Also, there is no sufficiency of any real defenses against them in particular with traditional security measures, which are listed above. [5] Thus, these countermeasures are still not enough to prevent all types of the DoS and DDoS attacks that target cloud computing. In particular, the X-DoS and H-DoS attack.

5. X-DOS AND X-DOS ATTACK

The cloud computing architecture consists of three models: Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS). These various services give cloud computing particularity than traditional networks. Cloud utilizes Service Oriented Architecture (SOA) and web services to introduce services that are accessible easily. Web services technologies and SOA are supported by SaaS for many business applications. When Cloud uses web services in SaaS, this leads to develop some vulnerabilities, which are exploited by attackers to launch X-DoS and H-DoS attacks. These types of attacks are easily implemented, but when they launch several times attacks, it is more difficult to prevent them. [4]

X-DoS attack uses an XML message that is sent to a Web Server or Web Service. This message includes malicious content to exhaust all their resources such as a Coercive Parsing attack, which exploits the Web Service Request. This occurs when a Simple Object Access Protocol (SOAP) is analyzed, which leads the content can be transformed to make it reachable to applications. The Coercive Parsing attack open XML tags by using continuous series, thus this exhausts CPU usage. When an attacker launches the X-DoS attack, this causes to flood the network with XML message rather than packets. Also, when the web server is flooded with XML requests, its services would not be available to users. Attackers can change the message content to disrupt the web server. [5]

H-DoS attacks are using a HTTP Flooder that starts up 1500 threads, it is able to send randomly a huge HTTP requests to a web server to use up all its communication channels. There is no method to differentiate between legitimate and illegitimate HTTP requests. [5]

5.1 Security Solutions against (X-Dos) and (H-Dos) Attacks

There are many Approaches to mitigate X-DoS and H-DoS attacks in cloud computing. However, I have chosen two different solutions, which are:

1. Based on what it was published by Ashley Chonka and her team [5], they proposed a protector depending on neural network to discover and filter X-DoS and H-DoS attacks by using:

   - Using Cloud TraceBack CTB to discover origin of an attack within a matter of seconds.
   - Using Cloud Protector (formerly known as X-Detector) to identify this form of attack and remove it from the system.

2. Based on what it was published by Reza Sarhadi and Vahid Ghafori [4], they proposed a solution by using their Cloud defender system called CSQD (Cloud Service Queuing Defender). It increases effective and efficient in detecting and remediying XML vulnerabilities in web services, can find a source of an attack, and learn from its experiment (self-learner) to avoid the same attack in the future.

6. CONCLUSION

The denial of services and the distributed denial of service attacks are the most challenging threats to the cloud computing. This paper takes listing the various these attacks, and discusses the mitigation of each attack. It takes into account the basic measures to ensure security the cloud systems. Thereby, these measures can safeguard the cloud systems from the most DDoS and DoS attacks. Further, this paper sheds some light on two types of the denial of service attacks, which are X-DoS and H-DoS. These types are the serious threat to the cloud system because of easy use and difficult to stop them. The defenses against these types are that using Cloud TraceBack CTB to identify source attack, and using also Cloud Protector to remove these types of attacks. Another solution is using the Cloud defender system (CSQD), which mitigates XML vulnerabilities in web services.

REFERENCES


