International Journal of Latest Trends in Engineering and Technology
Vol.(9)Issue(3), pp.167-169
DOI: http://dx.doi.org/10.21172/1.93.28
e-ISSN:2278-621X

A SECURITY APPROACH TO MANAGE ORGANIZATIONAL CLOUDS UNDER DOS ATTACK

Dr. Munindra Kumar Singh[1] & Mr. Prashant Kumar Yadav[2]

Abstract- Cloud computing is the fastest growing technology, which are adopted by many companies just like Amazon. But there are various security issues in cloud computing and one of them is DOS. It can effect organizations behavior and successful execution, depending on cloud for their business. This paper explains DOS attack, its effect in cloud computing and things needs to be considered while selecting defense mechanisms for DOS.
Keywords – DOS, AWS, EC2, Wireshark, OpenStack

1. INTRODUCTION

In 90's beginning of the global use of Internet, the fashion of a-lot-of computers accessing to one big server came back again. At that time web servers were required with plenty of power to hold the requests made from the Internet. From that time to current, more services are offered on Internet as well as more storage are need the users for their services.

At the end of the 90's, normally all data centres were using less than 10% of their capabilities because they wanted to reserve the rest for the occasional peaks, at that time Amazon made a great effort to solve this problem by adding capabilities by demand to the users, one of the concepts of Cloud Computing, fast and easy.

At 1999 Salesforce.com began to delivery services to enterprises by their own website and pioneered the concept of software as a service. In 2002 Amazon launched Amazon Web Services (AWS), a suite that includes storage, computation and others services. In 2006 Amazon launched Elastic Compute Cloud (EC2) to small companies and run their own computer applications in the cloud. In 2008, Eucalyptus was launched, being the first open source AWS API compatible platform for deploying private clouds. In 2009 Google began to offer enterprise applications based in browser as Google Apps.

Cloud Computing is a general term for anything that involves delivering hosted services over the Internet. It is being and forecasted that more and more users will rent computing as a service, moving the processing power and storage to centralized infrastructures rather than located in client hardware. This is already enabling start-ups and other companies to start web services without having to invest upfront in dedicated infrastructure. However, a major barrier for cloud adoption is real and perceived lack of security. Even though with multiple number of advantages, cloud is under high risk of attack and one such attack that can cause a major breach in security is DOS or DDOS attack.

2. OBJECTIVE OF THE RESEARCH PAPER

Since 2007, Cloud Computing has become hot issue; many companies began to attempt to use Cloud Computing services. The Cloud Computing has grown as a promising business concept as well as one of the fastest growing segments of IT industry in the last few years. The typical Cloud Computing service are Amazon's EC2 and Google's Google App Engine, they use the Internet to connect to external users, and take the large number of software and IT infrastructure as a service provided to users However the popularity of Cloud Computing is increasing day by day but there are some challenges that are faced by it. One of the main challenges of Cloud is security. With the fast growing of Cloud Computing technology, Data security becomes more and more important in it. In evaluating whether to move to Cloud Computing, it is important to compare benefits and also risks of it. From past few years, DDOS attacks have been placed first on the list of cloud attacks. DDOS can have serious consequences, especially on the companies dependent on the internet for their business. Thus, security and other existed issues in the cloud cause cloud clients need more time to think about moving to cloud environments.

3. METHODOLOGY

The objectives defined in the preceding section are achieved through the accomplishment of the following tasks:

- A thorough review of literature related to cloud computing and DOS attack.
- Analysis of detailed information and knowledge of the Cloud Computing, Virtualization and OpenStack which has been used in the implementation.

[1] Assistant Professor, Deptt. of Computer Application, UNSIET, VBSPU, Jaunpur
[2] Assistant Professor, Deptt. of Computer Science & Engineering, UNSIET, VBSPU, Jaunpur

- A literature survey to study one of the monitoring tools "Wireshark".
- All about the main drawback in the adoption of Cloud technology i.e. "Cloud Security". It contains the main concerns around Cloud Computing as well as the security threats faced by it. DOS attack and some existing methods for its detection have been discussed in this chapter. The proposed entropy based detection algorithm is also given
- The analysis of DOS attack shows that when dashboard was opened during the attack time period it took a longer time to load than normal which justifies that horizon was affected by the attack.
- The attack flow was monitored by using the Wireshark tool. The samples of attack flow can be collected and used to detect the DOS attack using the proposed Detection Algorithm.

4. SECURITY THREATS IN CLOUD COMPUTING

The following are the top security threats in cloud environment:

4.1 Basic Security

With the prevalence of latest technologies like Web 2.0 Security has become more important. The attacks observed over web are:

- SQL Injection attacks: These are the attacks in which an attacker gains an unauthorized access into the database through malicious code inserted into standard SQL code.
- Cross Site Scripting attacks: During this attack a malicious script is injected into web content and user considering it to be authentic executes it over its own machine, thus giving either control of the machine or exposure of confidential information to the attacker.
- Man in the Middle attack: In this attack an intruder enters in the ongoing conversation between sender and the receiver and makes them believe that conversation is taking place between them only.

4.2 Network level

Security Problems associated with networks are:

- DNS attacks: A Domain Name Server (DNS) server translates domain name into the IP address. Domain name are much easier to remember. But sometimes it happens that on calling a server by the domain name the user is routed to some other evil cloud.
- Sniffer attacks: It is a kind of application program which captures the packets flowing in the network and reads the information in it if it is not encrypted.
- Issue of Reused IP addresses: When a particular user moves out of a network his IP address is issued to another user. It may lead to security threat to the previous user because of time lag between the change of IP address in DNS and clearing of the IP addresses from the DNS caches. Thus, there are chances that the data of the previous user may become accessible by the new user.
- BGP Prefix IP addresses: The Internet relies on the Border Gateway Protocol (BGP) to convey routing information across Autonomous Systems (AS). As a BGP propagates the entire AS path is used to reach each destination network (represented by an IP address prefix). A hijacking of prefix takes place when a BGP router R announces a route to prefix P but R does not provide data delivery to P. Such a false router may appear more attractive to some other BGP routers than actual route to P. This influences routers to choose the route announced by R instead of actual route. The result of this would be that packets from the affected routers would be forwarded towards R instead of original destination, leading to serious privacy and security breaches.

4.3 Application Level Security

The threats to Application level Security are:

- Denial of Service attacks: A DOS attack makes services unavailable to an authorized user by flooding the server with the large number of requests.
- Cookie Poisoning: Cookie Poisoning attack involves manipulating and forging of the cookies used to achieve an unauthorized access to web application.
- Backdoor attacks: During the development of an application or Operating System program a backdoor is left intentionally by the developer for different purpose. These backdoors enable the normal authentication and gain access.
- Distributed Denial of Service: A DDOS attack is the one in which the collection of compromised systems attacks the target system. The targeted system thus denies the service to the authorized user.
- CAPTCHA Breaking: Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)'s were developed to prevent spam and over-exploitation of network resources by bots. But it has been observed that these CAPTCHAs can also be broken by the spammers.

5. REVIEW OF WORK

In 1960, John McCarthy proposed the term "public utility" which forms the underlying concept of cloud computation. First practise of the term "cloud" as a symbol of internet was published by MIT in 1996. At the starting of new century, IBM began to deploy new computing concepts like grid computing, pervasive computing, etc. In 2005, Amazon utility computing based services gave new direction to computing by modernizing their data centres.

Cloud Computing as defined in National Institute of Standards and Technology (NIST) highlights major aspects of cloud computing and gives actual meaning of clouds and mentions the strategies for using cloud computing at the best."

Statistical properties of normal and attack patterns can be exploited for detection of DDOS attacks. Generally a statistical model for normal traffic is stated and then a statistical inference test is applied to determine if a new instance belongs to this model. Instances that do not conform to the learnt model, based on the applied test statistics, are classified as anomalies.

Chen et al. developed a distributed change point (DCP) detection architecture using Change Aggregation Trees (CATs). The non-parametric "Cumulative Sum (CUSUM)" approach was adapted to describe the distribution of pre-change or post-change network traffic. When a DDOS flooding attack was being launched, the cumulative deviation was noticeably higher than random fluctuations. The CAT mechanism was designed to work at the router level to detect abrupt changes in traffic flows. The domain server used the traffic change patterns detected at attack-transit routers to construct the CATs, which represent the attack flow pattern.

Zhang et al. proposed a prediction method for the available service rate of a protected server by applying the Auto Regressive Integrated Moving Average (ARIMA) model. The authors have used available service rates to qualify the server's availability to detect DDOS attacks. Their prediction method divides server resources into CPU time, memory utilization and networking buffer. Based on the prediction, abnormal detection technology is used to analyze the consumption of server resources to predict whether the server is under DDOS attack.

6. REFERENCES

[1] James Staten, Simon Yates, Frank E. Gillett, and W. Saleh. (2008). Is Cloud Computing Ready For The Enterprise?

[2] Daryl C. Plummer, Thomas J. Bittman, Tom Austin, David W. Cearley, and D. M. Smith. (2008). Cloud Computing: Defining and Describing an Emerging Phenomenon.

[3] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities " presented at the 10th IEEE International Conference on High Performance Computing and Communications Dalian 2008.

[4] C. Yu, H. Kai, and K. Wei-Shinn, "Collaborative Detection of DDOS Attacks over Multiple Network Domains," IEEE Transactions on Parallel and Distributed Systems, vol. 18, pp. 1649-1662, 2007.

[5] J. Mirkovic, G. Prier, and P. Reiher, "Source-end DDOS defense," in Second IEEE International Symposium on Network Computing and Applications, 2003, pp. 171-178.

[6] Z. Yi, L. Qiang, and Z. Guofeng, "A real-time DDOS attack detection and prevention system based on per-IP traffic behavioral analysis," in 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), Chengdu, 2010, pp. 163-167.

[7] W. Jie, R. C. W. Phan, J. N. Whitley, and D. J. Parish, "Augmented Attack Tree Modeling of Distributed Denial of Services and Tree Based Attack Detection Method," in IEEE 10th International Conference on Computer and Information Technology (CIT) Bradford, 2010, pp. 1009-1014.

[8] C. Zhongqiang, C. Zhongrong, and D. Alex, "An Inline Detection and Prevention Framework for Distributed Denial of Service Attacks," The Computer Journal, vol. 50, pp. 7-40, 2007.

[9] H. Rahmani, N. Sahli, and F. Kammoun, "Joint Entropy Analysis Model for DDOS Attack Detection," in Fifth International Conference on Information Assurance and Security, Xian, 2009, pp. 267-271.