International Journal of Engineering Technology, Management and Applied Sciences

www.ijetmas.com February 2015, Volume 3 Issue 2, ISSN 2349-4476

Survey on DDoS Attack Detection and Prevention in Cloud

Patel Ankita
Fenil Khatiwala
Computer Department, Uka Tarsadia University,
Bardoli, Surat, Gujrat

Abstract: Cloud is becoming a dominant computing platform where chunks of data are kept online. Due to distributed nature of cloud they have become easy target to intruders to exploit information and necessity of data availability. Availability of data is most crucial part for economic growth of the society. Denial of Service (DoS) attack is an attempt to make network resource or requested data unavailable to its intended user by flooding the network by spoofing the IP. DoS attack is accompanied by IP Spoofing so as to hide the source of flooding and to make every request look different. However if malicious IP is kept similar throughout attack, it can be prevented. Distributed Denial of Service (DDoS), instead of using same IP throughout, it will broadcast packets to some compromised machine which will act as a bot and target the same network in synchronized way. This paper contains the survey about some of detection and prevention mechanism with their limitation.

Keywords: cloud computing, Distributed Denial of Service, DDoS attack.

1. Introduction

Cloud computing is an emerging new technology which provides a centralized pool of configurable computing resources and computing outsourcing mechanisms that makes available different computing services to different people. Advantages of cloud computing technology are cost savings, high availability, flexibility and easy scalability. As cloud is becoming the dominant part of the internet it is necessary for the vendors to keep them available throughout but due to cloud's distributed nature it becomes easy for intruders to intrude the system. Most dangerous attack over internet DoS whose aim is not to modify data or gain illegal access, but instead they target to flood the cloud and make it unavailable to their intended or legitimate users. Biggest problem in detecting DoS attacks is that the source address of the packets are spoofed. Due to spoofed packets attacker ensures that the compromised machines remain undetected and thereby can be used for other attacks. If the source of the attack is kept constant, then it is possible to block that particular address and stop the attack. But attack now takes a new form by being distributed. In this form, a number of compromised systems all over the world are used in such a way that they synchronically attack a particular target at the same time which makes flood on the targeted server. By distributing the attack, the intensity of traffic gets less on the source of attacker so it cannot be detected there. Meanwhile, the synchronically attack by multiple system at the same time at the victim is sufficient to overload networks and systems and thus they deny service to their legitmate users.

2. DDoS Attack in Cloud Environment

Distributed Denial of Service (DDoS attack) is a type of DoS attack, this kind of attack is an attempt to make a machine or network resource unavailable to its intended user. DDoS attacks are initiated by a network of remotely controlled nodes called Zombies [1]. Attacker launches the attack with the help of zombies and targets the single system to make its resource unavailable [1]. DDoS attacks are

www.ijetmas.com February 2015, Volume 3 Issue 2, ISSN 2349-4476

prone to Network and Cloud Infrastructure level threats [3].DDoS attacks generally target three kinds of resources Network Resource and Server Resource and Application Resource.

DDoS Attacks targeting Network Resources: This kind of attack attempt to consume all of a victim's network bandwidth by flooding the unwanted traffic to prevent the legitimate traffic from reaching the victim's network. Following are the two types of attack which targets the Network resources:

a) Flood attack: This attack is launched by an attacker sending huge volume of traffic to the victim with the help of zombies to jam the victim's network bandwidth with traffic [1].

b) Amplification Attack: This type of attack exploits the broadcast featured found in most of internetworking devices like routers. Attacker sends a large number of packets to a broadcast IP address. In turn the systems within the broadcast address range send a reply to victim resulting in malicious traffic at victim's network [1].

DDoS Attack targeting Server Resource: This kind of attack attempt to exhaust server's processing capabilities or memory. The idea behind this attack is to take advantage of existing vulnerabilities on the targeted server. Following are the two types of attack which target Server resources:

a) Protocol Exploit attack: This kind of attacks consume the excess amount of resource from the victim by exploiting the specific feature of the protocol installed in the victim [1]. TCP SYN attacks are the best examples of it.

b) Malformed Packet attack: In this packet is wrapped with malicious information or data. The attacker sends these packets to the victim to crash it. Example of this are IP Address attack and IP Packet options attack [1].

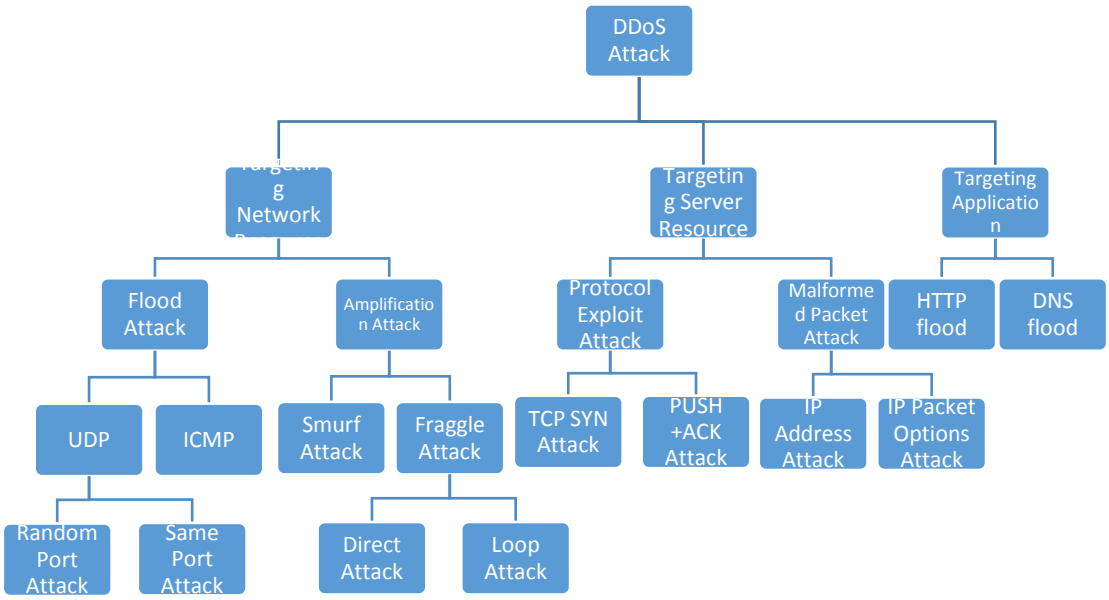

Fig. 2. 1 DDoS Attack Taxonomy

www.ijetmas.com February 2015, Volume 3 Issue 2, ISSN 2349-4476

DDoS Attack targeting Application: This kind of attack take advantage of the exploit found in the application protocol. They target not only the HTTP, but also HTTPS, DNS, SMTP, FTP, VOIP, and other application protocols which possess exploitable weakness.

3. Current Detection and Defense Mechanism

Usually by the time a DDoS flooding attack is detected, there is nothing that can be done except to disconnect the victim's cloud server from the network and manually fix the problem. DDoS flooding attacks waste a lot of resources of the targeted machine; hence, the ultimate goal of any DDoS defence mechanism is to detect attack as soon as possible and stop them [8]. Following are the few Detection and Defence mechanism discussed.

3.1 Dynamically resource allocation mechanism

This technique is designed for DDoS attack which target individual cloud customer. There are many access points between a cloud data centre and internet, where intrusion prevention system can be placed to monitor incoming packet. When cloud hosted server is under DDoS attack, this mechanism will automatically start allocate the idle resource of cloud dynamically to victim's machine which will assure the quality of service. Problem with this mechanism is that if cloud runs out of the idle resources no further allocation will take place, eventually DDoS attack will become effective. Hence, this solution can only be use as a short time defence against DDoS attack [2].

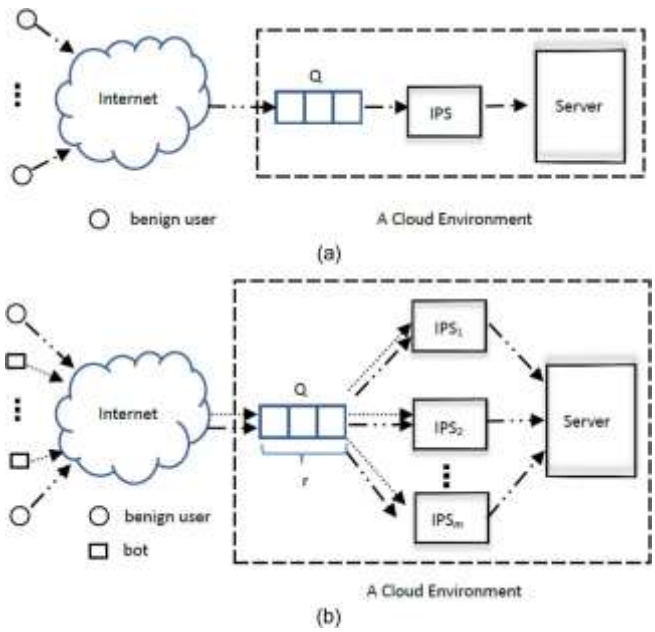

Fig. 2. 2 (a) Cloud hosted server in a non-attack scenario. (b) Cloud hosted server under DDoS attack with the mitigation strategy in place [2]

3.2 VM-Based Intrusion Detection System using Dempster-Shafer theory operations in 3-valued logic and the fault-tree analysis

In this technique VM-base IDS are created, by installing and configuring Snort into each Virtual Machine. IDS are used at VM to avoid overloading problems and to reduce the effect of possible attacks. IDS will generate alerts which will be further store into MySQL database which is present in

www.ijetmas.com February 2015, Volume 3 Issue 2, ISSN 2349-4476

cloud fusion unit. Using single database will reduce the risk of losing data. In addition to this improving capacity to analyse the result using Dempster-Shafer theory operations in 3 valued logic and the Fault-Tree Analysis for each VM-base IDS. This technique reduce the false alerts, increase detection rate and resolve conflicts generated by combination of information which are provided by multiple sensors [7].

3.3 Hop Count Filtering Approach

Hop count filtering technique is used to classify legitimate and spoofed packet. To compute hop count, TTL value in IP header is used. TTL is defined to prevent a packet from entering a routing loop. If TTL value becomes zero packet is discarded or else it will decremented by one. Therefore it is possible to calculate hop count from the value of TTL. Using HCF a mapping table IP2HC is created. But it is necessary to make legitimate entries to IP2HC table, to achieve that IP2HC mapping table should only be updated in established state of TCP connections. HCF will work in two phases Learning state and Filtering State [6]. Problem with this is there is lot of overhead in updating IP2HC table, because at every incoming packet it need to update IP2HC table. This algorithm continuous monitoring of packets travelling over network, hence it is also known as **packet monitoring technique**.

To reduce the overhead of this along with TTL field SYN flag of TCP header and source IP from IP header [4]. In this we need to extract SYN flag, TTL and source IP information from TCP/IP packets. The algorithm recognises four cases based on SYN and SRC which decide the updation of IP2HC table.

3.4 Filter Tree Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS attack

A filter tree approach was proposed by Karnwal to protect cloud against application layer attacks. Cloud defender is included five steps such as Sensor filtering, Hop Count Filter, IP Frequency Divergence, Double Signature and Puzzle Solver [9]. Problem with the filter tree approach is it lacks of practical application [3].

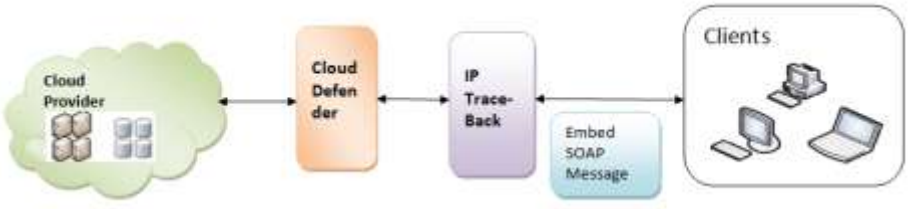

Fig. 2. 3 Filter Tree approach

4. Conclusion

Cloud computing is dominant part of today fast growing network over internet and availability is most important part of it. To keep the cloud available it is very necessary to provide Detection and Prevention mechanism for it. This paper provides different kinds of technique available for detection and prevention mechanism in brief but still DDoS attack is effective. The future work is to find a solution which can successfully detect and prevent DDoS attack in cloud.

www.ijetmas.com February 2015, Volume 3 Issue 2, ISSN 2349-4476

5. References

[1] B.Prabadevi, N.Jeyanthi, "Distributed Denial of service Attacks and its effects on Cloud Environment- a Survey", IEEE, 17-19 June 2014

[2] Shui Yu, Senior Member, IEEE, Yonghong Tian and Song Guo,, and Dapeng Oliver Wu, "Can We Beat DDoS Attacks in Clouds?", IEEE, 24 July 2013

[3] Issa M. Khalil, Abdallah Khreishah and Muhmmad Azeem "Cloud Computing Security: A Survey", MDPI

[4] Vikas Chouhan & Sateesh Kumar Peddoju, "Packet Monitoring Approach to Prevent DDoS Attack in Cloud Computing", International Journal of Computer Science and Electrical Engineering (IJCSEE) ISSN No. 2315-4209, Vol-1 Iss-1, 2012

[5] Jaswinder Singh, Krishan Kumar, Monika Sachdeva and Navjot Sidhu, "DDoS Attack's Simulation using Legitimate Attack Real Data Sets"

[6] Mr. I. B. Mopari, Prof S. G.Pukaleand Prof M. L. Dhore, "Detection and Defense Against DDoS attack with IP Spoofing", International Conference on Computing, Communication and Networking, 2008

[7] A.M. Lonea, D.E. Popescu and H. Tianfield , "Detecting DDoS Attacks in Cloud Computing Environment", 2006-2013 by CCC Publication

[8] Saman Taghavi Zargar, Jamesh Joshi and David Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE, 2013

[9] Tarun Karnwal, T. Sivakumar and G. Aghila, "A Comber Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS attack", IEEE, 1-2 March 2012