Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Detecting and Countering DDOS Attacks in Cloud

Baldev Singh, G.S. Samra
Lyallpur Khalsa College
Jalandhar, Punjab, India

S.N. Panda
RIMT
Mandi Gobindgarh, Pb., India

Abstract— This paper explored the possible issues predominantly concerning the cloud computing security environment in context of recent DDOS attack trends. This paper also includes how attack vectors may be measured and observed continuously so that the new tactics of DDOS attackers and malicious act service providers are countered. It discusses the way thresholds may be calculated wrong to inherent nature of the DDOS attack floods in various quarters of cloud based network, and finally the way in which these thresholds can be more accurately computed in terms of detecting overload congestion approaching due to malicious flood of packets leading to denial of services and request calls to target resource in a cloud.

Keywords— Cloud Computing, DDOS Attacks, Intrusion Detection, Scrubing Center, Attacks.

1. INTRODUCTION

There is an established underground cyber criminal economy which works to achieve their private individual goals best known for their keen interest in spying or for competitive monetary gains, motives that are possible by the use of disruptive technologies like DDOS attack. Thus making the science of DDOS attacks ever evolving and growing in current context in such a manner that a continuous monitoring with sophisticated watchdog capabilities is required as these attacks continues to create online outrages, customer inconvenience and reputational damages across all industries and geographies. The best known victims of recent moves of these DDOS attacks[4],5] and those who have been successfully being able to mitigate such attacks can never get a sound sleep as it is apparent from current incidences of this attack globally.

A recent attack on a cloud based online education site [1] was made target and DDOS attack leads to disruption of its services for more than business hours inspite of the fact that it had firewall protection with intrusion detection defense lines. The reason being that it was difficult to address as it was directed to the dedicated IP address rather than on the data centers as it was sourcing the malicious traffic that from diverse geographic sources. The attack became further intense with high sophistication tactics even after mitigation to secondary data center and were left with only one choice to either build a scrubbing center or hire a scrubbing center**.** As the primary work of the site is educational in nature, they were forced to get the services of the professional security experts and hire a scrubbing center [2].

2. SETTING UP OF SCRUBBING CENTER

Understanding the component of a scrubbing center is important here. It is however essentially a combination of software and hardware based algorithms recipes that analyze the incoming envelop of packets and check the integrity of the outgoing envelop of data passing through multiple subnets reaching a particular set of IP addresses. By scrubbing traffic at major Internet points and backbone connection, a defense line is created for mitigation of DDOS attacks. In fact they take advantage of bandwidth density and traffic routing options with globally distributed options. They choose more to change direction of traffic and swallow the volume of data rather than just block or filter the data packet as the difference between the good and malicious packet is difficult to assess. Hence, they are able to mitigate the flood of UDP [6,7] or any other type of traffic artifact creating DDOS attacks.

All cloud service providers can not afford to build their own scrubbing centers as they need to focus on their core business rather than technological issues of maintaining and defending themselves and moreover, even all cloud service providers can hire third party scrubbing solutions. Not all cloud service providers can maintain following components/processes with high quality and ensure high availability of services for themselves and their customers.

- Detection and Monitoring Centers.
- Threat correlation services.
- Threat alert system.
- Threat identification service with false positives recognition.
- Threat rate of change.
- Threat severity analysis.
- Threat heuristics at every layer.

Hence, when a centralized data cleansing stations are deployed having all possible capabilities as mentioned above where traffic is scrutinized and mischievous traffic (DDOS, known susceptibilities and exploits) are moved or absorbed, there is

normally an assumption that a volumetric attack bandwidth consumption can be overcome by adding more and more bandwidth, and swallow all data traffic thereby continuing the services, but it can happen for how much and how long is a question.

3. NEED OF SCRUBBING CENTERS TO COUNTER DDOS ATTACKS

Scrubbing centers having sophisticated processes that are often used in large enterprises, such as ISP and Cloud Service and Infrastructure Providers, and they often prefer to off-ramp traffic movement to an out of path integrated data cleansing location end-points. When under attack adversary, the whole traffic is redirected (typically using DNS or BGP) to the cleaning/scrubbing focal point where an attack mitigation system mitigates the attacks and passes clean data traffic back to the network for distribution system. The scrubbing center must be adequately equipped to sustain both low and high volumetric floods at the network and application layers, with RFC Compliance checks, with the known vulnerabilities and zero day anomalies addressed. These centers must be able to utilize a multiple diverse range of global network carriers, including Asian, American and European carriers to be really successful in building a defense line stretching beyond single set boundaries. Then, there are multiple ways in which workload management with respect to consolidation of the computing power and storage is done. Moreover, effectively partitioning of the computing capacity of the data centers into multiple tiers , which would improve the nodes utilization and responsiveness for parallel workload is a challenge more so , when there is a mix of solicited and unsolicited traffics of workload is coming into the data center, then the difficulty of realization of parallelism to monitor all ends of the data center effectively remains an issue , leading into a difficult condition in harnessing the heuristics of the scheduling algorithms in running the jobs of data center infected by malicious traffic until fully-meshed with redundancy for 100% availability is incorporated into the defense solution work to our advantage. Since , the target of the any DDOS attackers is normally to block or oversubscribe a resources in such a way that it leads to degraded service performance time , long response time matching the demand of processing the incoming workload remains a constant headache. Many methods have been evolved over a considerable time now and all these methods or technologies that claim to safeguard us from DDOS attacks also consider the various possible correlations that might be working to advantage of the attackers. The most common forces behind DDOS attacks are shown in the following figure [17]:

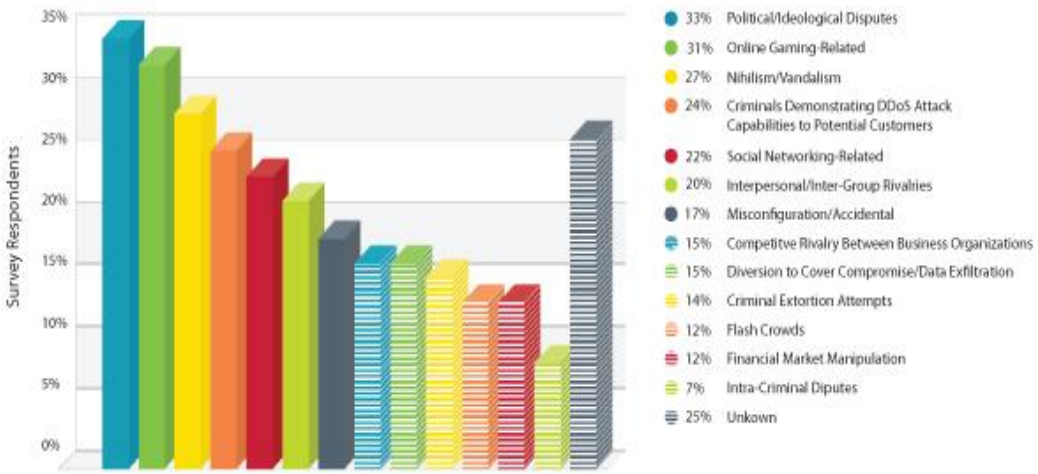

Fig.1: Common Forces behind DDOS Attacks

The following sections takes us to the point where we can now discuss the possible factors that must be observed, monitored and reported for synthesis of such attacks. However, it must be done by using multinational group of professionals with localized understanding of technical environment, cultures and practices to provide consultation and support in multiple languages to the customers so that DDOS attacks are thwarted with involvement of all the stakeholders of the network having protection scope which includes ICMP floods [4], UDP floods , SYN floods , application level floods , CC attacks [5,6,] , reflective attack[8] ,degradation of service attacks and last but not least unintentional DDOS outrage.

4. DDOS ATTACKS ASSESSMENT METRICS

Understanding what factors for thwarting DDOS attacks are needed to be monitored are, of course the starting point for any security expert, but measuring its vulnerability or proneness to attack with future predictability of attack is now the focus of most of the current algorithms. These algorithms are based on world recognized scoring systems which help to calculate the security fortification of IT infrastructure. The most popular scoring systems are Common Vulnerabilities and Exposure System and Common Vulnerabilities Scoring System. Both these systems attempt to measure of how much alarm a vulnerability warrants as related to the other known vulnerabilities and both the systems are point based systems where higher scores means that the known vulnerability need more attention in terms of plugging it and these systems runs on the reports from database of incidents occurring across the globe and ardently they give a contained picture of something going wrong in particular part of IT infrastructure based on the following main assessment parameters which cover almost everything when possibly a DDOS attack may occur. They include:

I. Access Vector (AV): This vector shows what magnitude of vulnerability may be exploited. It may occur in three possible ways as mentioned below:

(i) Locally: It is the factor which needs to measure when any malicious actor may either have physical access to the vulnerable piece of IT infrastructure. In context of DDOS attacks on cloud infrastructure, this is the access vector that is not exploited much as it cannot create mass service requests or flood of requests for a particular resource on Internet backbone by going to each physical piece of IT infrastructure e.g. cloud user device etc. However, the attacker may create DDOS attack having localized impact. It should also be noted that Common Vulnerability Scoring System system considers this access vector as one the base metric that measures the intrinsic qualities of the system in question, in fact, the next two vectors are also part of the base vector measurements also.

(ii) Adjacent Network: The malicious intended actor must have access to the broadcast or collision domain of the vulnerable system for example ARP spoofing may allow an attacker to capture data packet frames on a wired or wireless LAN, modify the traffic, or stop the traffic altogether. Again and again the attack is used as an opening for other attacks, such as denial of service, man in the middle, or session hijacking occurrences, therefore, in context of our focus in this research is on DDOS attacks that occur in cloud environment. Therefore this access vector measurement is important for the understanding of DDOS attack statistics.

(iii) Network Vector: This is the most critical assessment parameter in context of cloud computing environment where boundaries between networks of network are not crisp in nature due to inherent nature of the cloud infrastructure. In this context, this is a metric that measure the vulnerable interface working at layer 3 or above of the OSI Network stack and described as remotely exploitable (e.g. a remote buffer overflow in a network service). Since, many attacks were not designed to steal data nor are they were just another garden variety of DDOS attacks initiated to disrupt or embarrass.

Intentions of the attacks regarding DDOS attacks may be too malicious in nature and they may do harm to any extent, hence, we need an army of cyber defenders, to maintain business continuity. Further, more, it must be understood what the CVSS system does not do, it is not threat scoring mechanism nor a vulnerability database nor it is a way to classify the type of any vulnerability, it is in fact a way to find where to focus to plug in your vulnerability viz. locally, Adjacent Network or a Network.

II. Access complexity metric: The access complexity (AC) metric describes how easy or difficult it is to exploit the discovered vulnerability and is further classified as High, Medium and Low based on the difficulty in exploiting the vulnerability and in the context of the DDOD attacks. Since most the DDOS attacks are facilitated using scripts and bots and somehow these large number of scripts must be able to download themselves on geographically devise devices to orchestrate the DDOS attack floods. The first thing for the attacker is to find a way in the vulnerable server machines example, PHP web server. This cannot happen without understanding the complexity of the authentication and access complexity of the target which attacker is looking for, and if the authentication access complexity itself fails the attackers will have free hand in exploiting the device to their advantage.

High Level of Authentication access complexity here means that there is a specialized condition for authentication to be compromised which may be narrow window of opportunity. If we take a deeper look at the recent studies on the DDOS attacks, we will find that most the attackers success rate is high when the target servers are running on default settings that are well known to the intruders , hence it becomes question of some time that they are able to exploit these set of settings for example the protocol called CHARGEN was considered redundant some time back by system administration and most of the system administrator did not care much on its default settings in windows servers and it can be seen that there is a stream of malicious actors using this protocol for their ill advantage. However , if there are some additional requirements for access, such as a limit on the origin of the attacks, or a requirement for the vulnerable system to be running with an uncommon, non-default configuration it is considered to be Medium Level authentication and if there are no special difficult conditions for access to the vulnerability, such as when the system is available to large numbers of users, or the vulnerable configuration is ubiquitous, it is Low Access Complexity which is readily available for exploitation for the DDOS attackers .

III. Authentication vector: It is defined as the number of times the intruder must authenticate to finally get in or compromise the vulnerable system and it may be single time requirement to get into or it may require multiple times to get into the system. This attack vector metric is also critical when cloud network is suffering from a DDOS attack, as it requires cloud users' devices authentication for executing netbots scripts, stressors and other malicious scripts.

IV. Temporal Metrics vector: The business of capturing the real measure of the attacks is tricky business as the threat posed by vulnerability may go a change over period of time. Since Common Vulnerability Scoring System (CVSS) [9] seizures the confirmation of the technical details of a vulnerability, the remediation position of the vulnerability, and the availability of exploit code script or technical practices to overcome the issues it needs a continuous thought on the process of measure what and when, therefore, when certain metrics are not relevant for a particular attack statistics we can just keep that metric as temporal or simply miss it for considering for further synthesis and analysis.

V. Environmental Metrics: This metric measures the current state of exploit method or script obtainability. Public unrestricted accessibility of ease to use exploits code and increases the number of potential malicious actors and attackers by including those who are inexpert, thereby increasing the severity of the vulnerability for example, these days creation

and sale of scanning tools by underground vendors have been observed in the cyber gray market where it has been found that list of vulnerable servers is available with low cost option , and it is clear the underground vendors have moved from just providing list vulnerable ports list to more sophisticated in-depth details on the gaps/vulnerability of the networks .
Now DDOS attack services [17] are available at little cost options of merely five dollars. Therefore the overall environment is critical for the growth and blockage of such disruptive technologies. In the next sections, we shall look at the possible ways in which how we can detect and DDOS attacks. The Attackers are often watching every counter move and change their tactics on the fly, altering the use of infrastructure and application attack vectors and complicate the mitigation process.

I. 5. REVIEW OF TECHNIQUES USED FOR DETECTION OF ATTACKS AND ABNORMAL BEHAVIOR IN CLOUD

There are various studies that have explained the concept of solutions available for providing security with mitigation algorithms for cloud network, The Intrusion detection system (IDS) [15,16] are first to be debated and implemented as it is know fact the cloud based networks and services are prone to suffer from malicious attacks because of their inherent characteristics of being accessible globally any time and also due to the frequent changes in topology and development of Internet of things as well as because of landscape nature of Internet. Of particular concern, it is the denial of service attacks that makes the service unavailable to its intended cloud users.
As per our systematic review of related works in the field of intrusion/malicious attack detection, there are many techniques which can be used to detect intruders or malicious behavior in the cloud network. Each of these techniques/frameworks holds their own merits and demerits. In fact, there are three major techniques which are: misuse detection, anomaly detection and specific detection like DDOS attack. However, to understand this field we must look at what each technique holds in its favour and what trade-offs it must make to achieve its goals in case of using some threshold technique for identification of abnormal behavior which seems to be DDOS at first glance.

Static Thresholding Method: In this method, the factor that is most critical for the identification of the DDOOS attack is monitored based and any action to mitigate the issue is done based on pre-selected value for that metric, for example, these algorithms detect the CPU utilization overload pattern based on fixed or pre-determined value and if the value is greater than some x threshold then it is considered to be behaving in abnormal way.
Merits: Absolute threshold values easy to implement for detection, Low computational complexity.
Demerits: Fix value range is never close to real systems that changing every day, this method will never be able consider differential or cumulative threshold for giving response to adversity in real time.[10].

Dynamic Thresholding Method: In this method the value of upper and lower limits are calculated for the factor which is most significant for detection of the DDOS attack. There limits [thresholds] are calculated based on some logic depending standard deviation etc.
Merits: Not much difficulty e.g. method based on average, mode, frequency.
Demerits: Statistically cannot handle extreme high and low values may lead to wrong calculations of mean, change point detection method may calculate wrong threshold , thereby increase the false alarm rate especially distributed change point detection.[DFA or deviation from Average][11].

Single Range Thresholding Method: In this method the single value is calculated either dynamically or based on heuristics of the all the factors important for detecting the DDOS attack and if this value is less than or greater then a particular agreed standard it is classified as abnormal and normal behavior.
Merits: Easy and simple to implement, clear cut demarcation of normal and abnormal behavior events in cloud network with upper and lower limit, methods include local regression etc.
Demerits: Dynamic systems like cloud or adversity causing systems cannot work on such single range threshold and detection decision making may be faulty. Probability based classification may work and correlation necessary to really reach accurate single range threshold technique [12].

Multi –Range (static) Thresholding Method: This method basically does not calculate the thresholds dynamically based on the current statistics, it works on the multiple range thresholds which are either based on predetermined on service level agreements or may be based on descriptive statistics calculated in recent past of the factor which can help us detect the DDOS attack .
Merit: Simple to implement, clear cut demarcation of normal and abnormal behavior events in static upper and lower limit Methods in inter quartile range.
Demerits: Dynamic systems like cloud or adversity causing systems cannot work on such muti-range threshold systems as the range may be discrete or continuous and may be changing with time [13].

Multi –Range (Dynamic) Thresholding Method: As mentioned above in case of static multi range thresholding method , this method calculates all the factor multiple infection points for taking decision on what traffic is malicious and normal based on current dynamics and heuristics .
Merits: Methods include X-bar , R-bar , Control limit charts based on variance , standard deviation etc.
Demerits: Difficult to calculate accurately as ranges may changing with pattern difficult to comprehend and range may be discrete in nature [14].

Although considerable efforts have been made to understand, detect and prevent these attacks, yet because of continuous evolving nature of cloud we have to remain on our toes and try to find out means and tools which can eliminate this malicious threat. Since it is a continuously evolving as technology, new ways are found by anti-development sources to compromise the cloud based systems, therefore methods that are based on single, multi range thresholds for detection need constant upgradation as well refinement in terms of the algorithms accuracy and robustness for identification of DDOS attacks. The threshold based algorithms for detection of DDOS attack must always numerically stable as well as must not depend on predefined thresholds.

The current intrusion detection systems mentioned in the previous works [15] overlook certain aspects of calculating the threshold for identification of subspace set of abnormal behavior with the whole pattern of VM profile and this is based on frequency calculation happening in particular set of time line, which is not capable of further mathematical treatment or insight and it is more useful in qualitative cases, however, it makes more sense, if relative frequency based threshold could have been used which would have also considered the total outcome of normal and abnormal events in the VM profile. It would be more accurate to consider those methods that would fine in extreme cases when values are either too large or too small or the dataset is skewed due to particular pattern of events.

Therefore, we propose variance based methods that can be used to overcome the demerits of existing solutions, calculate the thresholds more accurately and to achieve our objective of research. Hence, In pursuance of this research work it must be persuaded by all the stake holders to analyze methods that can deal with large skewed datasets ([benign traffic] to abnormal behaviour [malignant traffic] for detection of DDOS attacks, since the thresholds cannot be static in nature in any way in cloud environment for parameters that are critical to analyze for identification of DDOS Attacks.

6. CONCLUSION

From the systematic review of all the studies done in the context of the DDOS attack we can see that there will be increase in the frequency of the DDOS attack due to multifold increase in the online, wireless Internet of things and it is also very clear that the very idea of building defending lines of action against such act of destruction depends on computations coming out of the stream of the traffic at different ends of the network of networks. We have also understood that both the internal and external anatomy of the data center matters, how it is structured architecturally to measure the volume of traffic is the main critical point, if somehow the intruders are able to launch a slow attack it must be detectable or if it is a sudden flood of packets then we must be able to mitigate the flood to have clean traffic. This is not possible unless we have continuous monitoring which includes the mapping of threats cope with the understanding correlations of all the factors contributing to the adversary. Therefore, the thresholds of finding inflection points where the traffic changes to malicious is essential to successful running of data centers in cloud in thwarting the DDOS attacks .

REFERENCES

[1] **John Breeden II , GCN Lab, http://gcn.com/Articles/2013/10/22/DDoS-attacks.aspx**

[2] **http://www.ddosattacks.biz/ddos-101/glossary/scrubbing-center/**

[3] **Song Ning; Qiu Han, "Design and implementation of DDoS attack and defense testbed," Wavelet Active Media Technology and Information Processing (ICWAMTIP), 2012 International Conference on , vol., no., pp.220,223, 17-19 Dec. 2012 doi: 10.1109/ICWAMTIP.2012.6413478**

[4] **Udhayan, J.; Anitha, R., "Demystifying and Rate Limiting ICMP hosted DoS/DDoS Flooding Attacks with Attack Productivity Analysis," Advance Computing Conference, 2009. IACC 2009. IEEE International , vol., no., pp.558,564, 6-7 March 2009 doi: 10.1109/IADCC.2009.4809072**

[5] **Xie Chuiyi; Zhang Yizhi; Bai Yuan; Luo Shuoshan; Xu Qin, "A Distributed Intrusion Detection System against flooding Denial of Services attacks," Advanced Communication Technology (ICACT), 2011 13th International Conference on , vol., no., pp.878,881, 13-16 Feb. 2011**

[6] **"CERT Advisory: SYN Flooding and IP Spoofing Attacks," CERT® Coordination Center Software Engineering Institute, Carnegie Mellon, 2010. http://www.cert.org/advisories/CA-1996-21.html**

[7] **Xia Chun-Tao; Du Xue-Hui; Cao Li-Feng; Chen Hua-Cheng, "An Algorithm of Detecting and Defending CC Attack in Real Time," Industrial Control and Electronics Engineering (ICICEE), 2012 International Conference on , vol., no., pp.1804,1806, 23-25 Aug. 2012 doi:10.1109/ICICEE.2012.477**

[8] **Bao-Tung Wang; Schulzrinne, Henning, "An IP traceback mechanism for reflective DoS attacks," Electrical and Computer Engineering, 2004. Canadian Conference on , vol.2, no., pp.901,904 Vol.2, 2-5 May 2004 doi: 10.1109/CCECE.2004.1345260**

[9] **Scarfone, K.; Mell, P., "An analysis of CVSS version 2 vulnerability scoring," Empirical Software Engineering and Measurement, 2009. ESEM 2009. 3rd International Symposium on , vol., no., pp.516,525, 15-16 Oct. 2009 doi: 10.1109/ESEM.2009.5314220**

[10] **Research Papers Referred: Faizal M.A., and Zaki M.M., and Shahrin S., and Robiah Y., and Rahayu S.S., (2010) Statistical Approach for Validating Static Threshold in Fast Attack Detection. Journal of Advanced Manufacturing.**

[11] **Research Papers Referred: A Profile Based Network Intrusion Detection and Prevention System for Securing Cloud Environment Sanchika Gupta,1 Padam Kumar,1 and Ajith Abraham2,3,2013**

[12] **Research Papers Referred: User Profiling for Intrusion Detection Using Dynamic and Static Behavioral Models, Dit-Yan Yeung, Springer Berlin Heidelberg, 2002 Yuxin Ding**

[13] Shicong Meng; Iyengar, Arun K.; Rouvellou, I.M.; Ling Liu; Kisung Lee; Palanisamy, B.; Yuzhe Tang, "Reliable State Monitoring in Cloud Datacenters," Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on , vol., no., pp.951,958, 24-29 June 2012doi: 10.1109/CLOUD.2012.10

[14] http://www.carbon60.com/the-truth-about-ddos-attacks-part-1/ Nov. 21, 2013.

[15] Vasanthi, S.; Chandrasekar, S., "A study on network intrusion detection and prevention system current status and challenging issues," Advances in Recent Technologies in Communication and Computing (ARTCom 2011), 3rd International Conference on , vol., no., pp.181,183, 14-15 Nov. 2011 doi:10.1049/ic.2011.0075

[16] B. B. Gupta, R. C. Joshi and M. Misra, "Defending against Distributed Denial of Service Attacks: Issues and Challenges," Information Security Journal: A Global Perspective, Vol. 18, No. 5, 2009, pp. 224-247.

[17] S. M. Specht and R. B. Lee, "Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures," Proceedings of the International Workshop on Security in Parallel and Distributed Systems, San Francisco, 15-17 September 2004, pp. 543-550.

