INTERNATIONAL JOURNAL OF ENHANCED RESEARCH IN MANAGEMENT & COMPUTER APPLICATIONS
VOL. 2, ISSUE 2, FEB.-2013 ISSN NO: 2319-7471

Analysis of the DDoS Defence Stratigies in Cloud Computing

Amit Khajuria[1], Roshan Srivastava[2]
[1]M. Tech Scholar, Computer Science Engineering, Lovely Professional University, Punjab, India
[2]Asst. Prof., Computer Science Engineering, Lovely Professional University, Punjab, India
[1]amitkhajuria8@gmail.com, [2]roshan.1686@lpu.co.in

Abstract: Cloud computing emerges as a potential technology for the future and expanding on one of the principles of utility computing is often claimed to represent a completely new paradigm for viewing and accessing computational resources Distributed Denial of Service (DDoS) is an attack that threats the availability of the cloud services . It is necessary to analyze the fundamental features of DDoS Defence stratagies. This paper provides certain strategies that been implemented to the DDos attack. These strategies are defined in these paper and use of technologies for different kind of of malfunctioning in the cloud.

Keywords: DDoS, Entropy, CLAD, IDS.

I. Introduction

DDoS may be called an advanced version of DOS in terms of denying the important services running on a server by flooding the destination sever with a large number of packets such that the target server is not able to handle it. If an attacker mounts an attack from a single host it would be classified as a DoS attack. In fact, any attack against availability would be classed as a Denial of Service attack. On the other hand, if an attacker uses many systems to simultaneously launch attacks against a remote host, this would be classified as a DDoS attack .The attackers have the power to control the flow of information by allowing some information available at certain times. Since the extent of damage by DDoS attacks has increased, many studies on the detection mechanism have been carried out. However, the existing security mechanisms have failed to provide effective defence against these attacks or just can only provide defence against specific types of DDoS attacks. Some DDoS attack detection methods are based on traceback, while others are based on feature monitoring of a router or a server. However, existing methods have limited success because they cannot simultaneously achieve the objectives of efficient detection with a small number of false alarms and realtime transfer of all packets. For instance, some methods, which apply data mining techniques, can obtain a high correction rate in detecting the attacks. However, these methods usually can't be employed in real-time computing. Other methods, exploiting the abnormal increase in some types of packets, mitigate only some types of DDoS attacks. Furthermore, presently, there exist few effective and detailed model frameworks available for the detection and prevention of DDoS attacks**.** The detection of DDoS attacks is usually studied from three different perspectives:

1) Near the victim
2) Near attack sources
3) Within transit networks.

The major advantages to an attacker of using a distributed denial-of-service attack are that: multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behaviour of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms.

DDoS Attack Classifications

There are two main classes of DDoS attacks: bandwidth depletion and resource depletion attacks. A bandwidth depletion attack is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the victim system. A resource depletion attack is an attack that is designed to tie up the resources of a victim system. This type of attack targets a server or process at the victim making it unable to legitimate requests for service.

VOL. 2, ISSUE 2, FEB.-2013 ISSN NO: 2319-7471

DDoS Characteristics

There are several features of DDoS attacks that hinder their successful detection and defence

- DDoS attacks generate a large volume flow to the target host. The victim cannot protect itself even if it detects this event. So the detection and defence of DDoS should ideally be near the source of the attack or somewhere in the network.

- It is difficult to distinguish attack packets from packets. Attack packets can be identical to legitimate packets, since the attacker only needs volume, not content, to inflict damage.

- DDoS traffic generated by available tools often has identifying characteristics, making the detection based on possible analysis.

II. Defence Against DDos Atacks

1). CLAD (Cloud-Based Attack Defence)

CLAD run on cloud infrastructures as a network service to protect web servers. Their goal is to make an innovative DDOS defense solution which have enough capacity to exceed the firepower of the botnets. CLAD is a fully transparent solution that requires no modifications to client-side and server software. As an improvement, a CLAD system can be designed as an ondemand system when the server-side is equipped with some attack detection system The defense shared thousand of hosts to increase the system utilization. The main thingh about CLAD is that the protected server is hidden from internet. All traffic to the protected server is forwarded through at least one CLAD node, which verifies the clients and relay the requests. The CLAD nodes exchange their healthy status with neighbors by fetching a special small file periodically CLAD works efficiently but the CLAD node can not distinguish between malicious packets and configure the firewall to ask the cloud to filter unwanted packets.

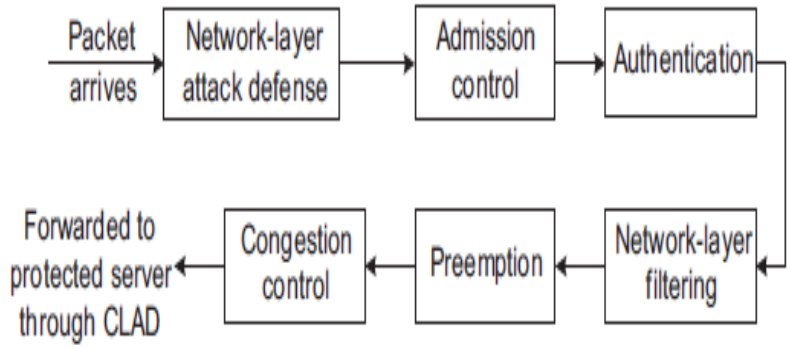

Fig. 1: Control Mechanism of CLAD

2). Transparent and Intelligent Fast-Flux Swarm Network

It is an effective DDOS technique consisting of nodes in swarm network and try to mitigate DDOS attacks with transparent and intelligent Fast-Flux swarm network. It uses IWD (Intelligence Water Drop) mechanism. The client tries to reach the server through a fully qualified domain name. The client is directed to the server and then sends its request to the designated server. The server then responses and the result is forwarded to the client. There are certain limitations in their approach. The swarm network binds each client to a server through a unique route that exists only for a particular connection. Each message will pass through a unique route that is not guaranteed for the next transmission. It is one time use only. The route changes according to the varying network. It doesn't allow SSL connections to possible. Moreover, fast changes in the swarm network result in inactive name servers listed.

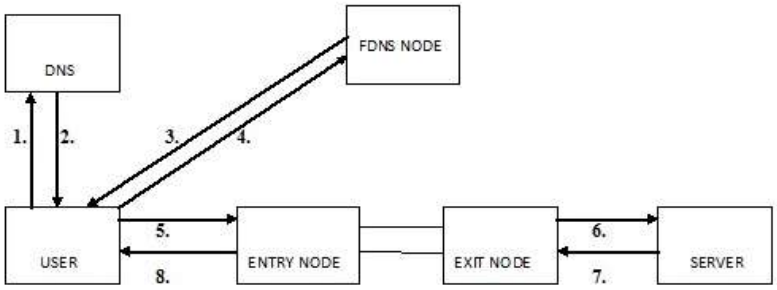

Fig. 2: Operation of relay mechanisms

1. User contacts ISP DNS server to find designated Nameserver for swarm network.
2. DNS returns FDNS address.
3. User DNS resolution request to the FDNS.
4. FDNS returns the address of an entry node.
5. User sends request to entry node, perceiving it as server itself.
6. Exit node sends the request to the server.
7. Server sends the response to the exit node.
8. The entry node relays the response back to the user.

3). IDS (Intrusion Detection System)

Intrusion Detection is like a game of chess. ID software to date commonly analyzes the actions of an attacker in more or less linear, this stream of packets matches a stream known to be a smurf, SYN, or other known attack signatures. Signature-based ID systems are adequate to deal with misuse intrusions, but can't deal with out-of-the-box thinkers who pen-test, audit, or attack networks, purposely thinking non-linearly with the expectation of ultimately discovering code, policy, and logic flaws. IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. They also can't adequately deal with anomalous behaviors and results intrusions, e.g., the disgruntled insider who abuses authorized access, the unwitting user who is victimized by a worm, the server that is back door.

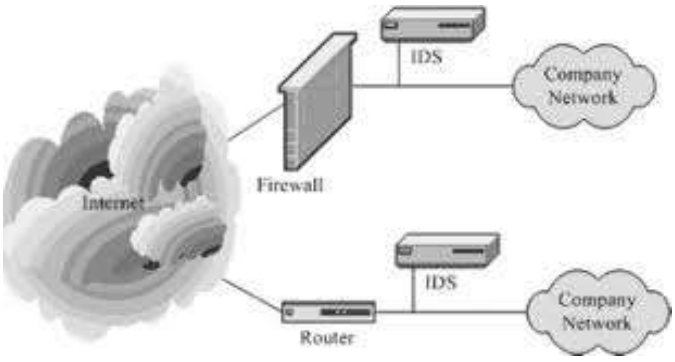

Fig. 3: IDS working parameters

4). Machine Learning Automatic Defence

It detects network anomalies and find the attack traffic according to the trained neural network. When the attack is confirmed, those packets with specific marks as the attack packets are filtered out. We test the incoming packets by the

trained neural network. If the output indicates anomalies, we further investigate the composition of marked packets. If the number of packets that have the same address digest bits exceeds a threshold N drop (this value is decided by experience), this flow of packets will be filtered. Here flow means the packets have the same destination IP address and digest bits. This two-step design can not only protect legitimate traffic that shares a large portion of bandwidth but also punish entirely the attack traffic. First, because the anomaly detection is performed by a nonlinear neural network classifier with the assistance of concentration of the packets of same digest bits, the legitimate traffic will be less likely decided as an anomaly than by other coarse granite classifier such as statistical model. Second, once the attack traffic flow is identified, this flow can be totally filtered by differentiating the identity – digest bits that FDPM marks.

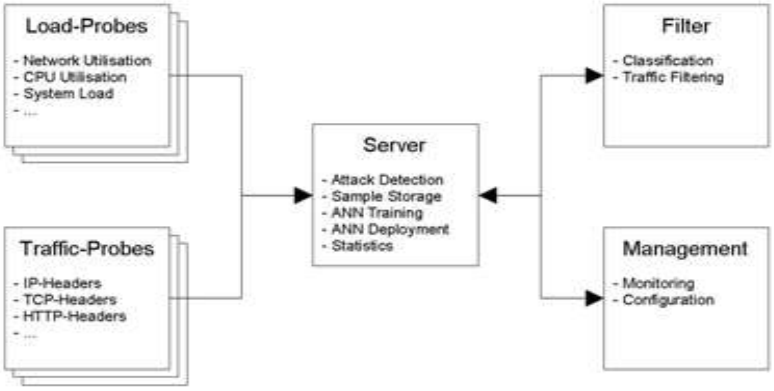

Fig. 4: Machine Learning Automatic Defence

5) Auto- Responsive Honey Pot Architecture

It is an appropriate approach to defend DDOS attack in form of integrated auto-responsive framework that aims to restrict attack flow reach target and maintain stable network functionality under attack network. It is a combine detection and characterization with attack isolation and mitigation to recover networks from DDOS attacks. It leads the attacker to believe that they are succeeding in their attack, whereas they are simply wasting time and attack never occurs. Their architecture presented an end to end solution for defense against degrading and high rate concentrated flooding DDOS attacks in ISP domain. It is a favourable attack load independent behaviour for fixed number of attack machines and self optimize the detection. Honeypots help in retaining attack evidence for forensic purposes and enable smooth operation even under heavy load. It dynamically adapts its offered services and resources to meet changing network demands. It uses reasoning to optimize its behavior and policy-based management to govern the behavior of the control loop . Since there are no bulky update in the messages, there is less bandwidth overheads in terms of control traffic exchanged between defense modules. There is great improvement in throughput of the security mechanism but for the high traffic rate there are still problem.

6) Data-Mining Approach

A combined data mining approach for the DDoS attack detection of the various types, that is composed of the automatic feature selection module by decision tree algorithm and the classifier generation module by neural network. IT gathered the real network traffic in the normal case and the attack case. It can mounted the most powerful DDoS attack changing attack types, so it can tackle with the attack traffic of various types. And used the NetFlow data as the gathering data, because the analysis per flow is useful in the DDoS attack detection. Because the NetFlow provides the abstract information per flow, we don't need the extensive pre-processing, different with the tcpdump. It uses the automatic feature selection mechanism and builds the classifier by the neural network technology with the automatic selected attributes. For the selection of the important attributes, heuristic method can't prove that the choice is the best, and the many trials and the many processing time are required.

7) K-NN Classifier

K-NN classifiers is an efficient appreoach to detect DDoS attacks and classify the network status to the classes. K-NN can consider the classification of the current network status to one of the classes. There are many well-known methods for classifying documents such as SVM, NN, fuzzy logic, and rough set .The k-NN method has features that are suitable for detecting smaller DDoS attacks. These features are: easy implementation, short time computation, and high accuracy. The k-NN algorithm is a similarity-based learning algorithm and is known to be highly effective in various problem

domains, including classification problems. The k-NN algorithm finds its k nearest neighbors among the training elements, which form the neighborhood of the Majority voting among the elements in the neighborhood is used to decide the class for dt. This approach is often referred to as a nearest neighbour classifier. The downside of this simple approach is the lack of robustness that characterize the resulting classifiers. The high degree of local sensitivity makes nearest neighbour classifiers highly susceptible to noise in the training data The term 'near' can be defined as the degree of similarity between two elements. There are several techniques to compute the similarity degree between two elements. However, the algorithm based on the cosine formula is most popular method used for estimating the similarity degree.

8) DDos Detection using Entropy

The entropy algorithm first builds a profile of the network's normal behaviour monitored at selected networks nodes, in the absence of any attack [4]. In fact given a certain PSN setup (i.e. topology, routing algorithm, and source load) a natural level/value of entropy, a sort of "fingerprint" of the given PSN setup, characterizes normal PSN operation, i.e. normal traffic. Whenever, the entropy deviates from this profile, it means that some PSN traffic anomaly is emerging. Detecting shifts in entropy in turn detects anomalous traffic and, in our virtual experiment, a ping DDoS attack. DDoS attacks change natural spatio-tempral packet traffic patterns, i.e. natural distributions of packets among routers.These changes may be detected by calculating entropy of packet traffic monitored at a small number of selected routers [4]. Thus, one can detect anomalies in packet traffic using entropy based detection methods because the values of entropy of packet traffic sharply decrease from the "fingerprint" profiles shortly after a start of DDoS attack, meaning with certainty presence of an infrequent event, i.e. an emerging anomaly in packet traffic. In our simulations these anomalies were caused by ping DDoS attacks. Our simulations show that the ability to detect changes in entropy of packet traffic monitored at selected number of nodes during DDoS attack depend on the number of these monitoring nodes and the type of routing algorithm being used. It is much easier to detect DDoS attack for static routing than dynamic ones. In the case of dynamic routings the entropy based detection is much more sensitive to the location of the monitoring nodes if their numbers are small in comparison with the network size and additionally DDoS attack is weak. We have observed that strong DDoS attacks cause significant and almost immediate changes in entropy of packet traffic monitored even at a small number of routers regardless of their position and type of routing algorithm used by PSN model. Thus, entropy provides promising tool to detect DDoS attacks. However, several questions need to be explored further, i.e. how to select the monitored routers and how many of them so that entropy can detect anomalous packet traffic regardless of its intensity**.**

Conclusion

Distributed denial of service is a major threat that cannot be addressed through isolated actions of sparsely deployed defence nodes. Instead, various defence systems must organize into a framework and inter-operate; exchanging information and service, and acting together. A strategy must be propoed that defend DDoS attack even in high data flow. Intermediate should be applied to the network for more security of the network. IDS withe the intermediate node can be used over the overlay network to provide efficient security to the cloud. DDoS is a serious threat to the devolping infrastructure in the recent environment and must be defend in the payment gateways. .

References

[1]. Weiss A, "Computing in the Clouds. Networker", 11(4), 16-25, 2007.
[2]. Vidyanand Choudhary, "Software as a service: Implications for Investment in software development", hicss, pp.209a. 40th Annual Hawaii Int. Conf. Sys. Sci. (HICSS'07), 2007.
[3]. Bhaskar Prasad Rimal, Eunmi Choi, Ian Lumb, "A Taxonomy and survey of cloud computing sytems", Ncm. 5th Int. Joint Conf. INC, IMS & IDC. pp.44-51, 2009.
[4]. Ian Foster, Yong Zhao, Ioan Raicu and Shiyong Lu, "Cloud computing and grid computing 360-Degree compared", IEEE Grid Comput. Environ.(GCE08) 2008, co-located with IEEE/ACM Supercomputing, 2008.
[5]. Luis M Vaquero, Luis Rodero-Merino and Daniel Morán, "Locking the sky: a survey on IaaS cloud security", Comput. 91(1), 93-118, 2011.
[6]. Cloud Computing Incidents Database, World Wide Web, http://wiki.cloudcommunity.org/wiki/CloudComputing: Incidents_Database.
[7]. Amazon Web Services Discussion Forums, World Wide Web, http://developer.amazonwebservices.com/connect/thread.jspa?threadID=21401&tstart=15.
[8]. Rachael King, "How Cloud Computing Is Changing the World", In Businessweek on the World Wide Web, http://www.businessweek.com/technology/content/aug2008/t c2008082_445669.htm. Aug 4, 2008.
[9]. Cloud Security Alliance, World Wide Web, http://www.cl oudsecurityalliance.org.
[10].J. Oberheide, E. Cooke, and F. Jahanian. "CloudAV: NVersion Antivirus in the Network Cloud", In the Proc. of the 17th USENIX Security Symposium. July 2008.