International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 4, Special Issue
September 2015

Distributed Denial of Service(DDoS) Attack Techniques and Prevention on Cloud Environment

Keyur Chauhan[1],Vivek Prasad[2]
[1]*Student, Institute of Technology, Nirma University (India)*
[2]*Assistant Professor, Department of CSE, Institute of Technology, Nirma University (India)*

ABSTRACT

Cloud computing has been considered as one of the great importance and emerging networking technology, which has been changed the era of computing in last few years. Despite the security concerns of protecting data or providing continuous service over the cloud, many organisations are considering different types cloud services as potential solution for their business. We are researching on cloud computing security issues for cloud service providers. Researchers have demonstrated that the extremely important issues of Distributed Denial of Service (DDoS) attack and defense are the resource competition between the attackers and defenders. A cloud usually have profound resources and has full control and dynamic allocation capabilities. Therefore, cloud offers us the potential to overcome DDoS Attack. We propose a cloud-enabled defense mechanism for Internet services against DDoS attacks.

***Keywords*: DDoS Attack, Techniques of DDoS Attack, Cloud Security, Mitigation, Network Security.**

I. INTRODUCTION

A Denial of Service (DoS) attack is an attack with the purpose of preventing legitimate users from using a specified network resource such as a website, web service, or computer system [1] . A Distributed Denial of Service (DDoS) attack is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems.

DDoS attacker may use thousands of different IP addresses to send different types of data packets to the targeted server or network. The process becomes very complicated for the victim server or network to differentiate between the legitimate traffic and “fake” traffic. Situations become more complicated when the attackers use spoofed IP addresses as a source to send the packets, which make it difficult to identify the origins of attacks. The DDoS attack can cause significant business loss because of less productivity and services, increase downtime; therefore loss in reputation. There are two main reasons that make DDoS attack very popular among different groups of users. Firstly, there are many tools available to conduct DDoS attack on the victim. Most of these tools can be used by attacker without having a great deal of technical expertise[2]. Availability of worm maker and ignorance of a large number of Internet users make it convenient for attacker to place “bot” into different computers, what can be used for DDoS attack. Secondly, victim organisation will have to spend time and resources to locate attacker, which needs significant involvement of IT security experts. Many organisations are not ready to spend adequate amount of resources to investigate the source of the attack, which encourages the attacker to conduct an attack. Because of the high risk of losing company reputation, number of companies tries not to disclose any security incident in public, which also motivates the attacker to use this technique.

In Section 2 we describe classes of DDoS attack architectures. In Section 3 we present techniques for DDoS attacks. In Section 4 we present the prevention technique. We conclude in Section 5.

2. DDoS Attack Architecture

There are two types of DDoS attack networks have emerged: The Agent-Handler model and the Internet Relay Chat (IRC)-based model.

The Agent-Handler model of a DDoS attack present of clients, handlers, and agents (Figure 1). The client is where the attacker communicates with the rest of the DDoS attack system. The handlers are software

packages located throughout the Internet that the attacker's client uses to communicate with the agents. The agent software exists in compromised systems that will eventually carry out the attack. The attacker communicates with any number of handlers to identify which agents are up and running, when to schedule attacks, or when to upgrade agents. The owners and users of the agent systems typically have no knowledge that their system has been compromised and will be taking part in a DDoS attack. Depending on how the attacker configures the DDoS attack network, agents can be instructed to communicate with a single handler or multiple handlers. Usually, attackers will try to place the handler software on a compromised router or network server that handles a large volumes of traffic. This makes it harder to identify messages between the client and handler and between the handler and agents. In descriptions of DDoS tools, the terms "handler" and "agents" are sometimes replaced with "master" and "daemons", respectively.[3]

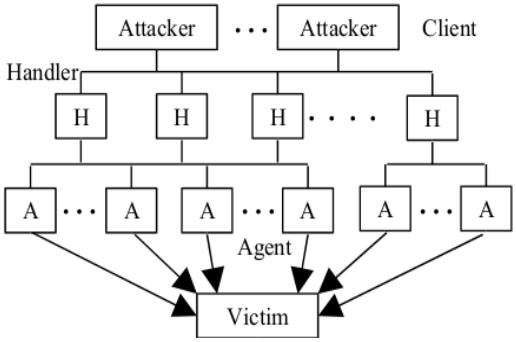

Fig. 1: DDoS Agent-Handler Attack Model

Fig. 2 : IRC Based DDoS Attack Model

The IRC-based DDoS attack architecture is similar to the Agent-Handler model except that instead of using a handler program installed on a network server, an IRC (Internet Relay Chat) communication channel is used to connect the client to the agents. An IRC channel provides an attacker with additional benefits such as the use of "legitimate" IRC ports for sending commands to the agents [4] . This makes tracking the DDoS command packets more difficult. Additionally, IRC servers tend to have large volumes of traffic making it easier for the attacker to hide his presence. Another advantage is that the attacker does not need to maintain a list of the agents,since he can log on to the IRC server and see a list of all available agents [4] . The agent software installed in the IRC network usually communicates to the IRC channel and notifies the attacker when the agent is up and running.

3. Techniques DDoS ATTACK

There are a wide variety of DDoS attacks. We propose a techniques of the DDoS attack methods in

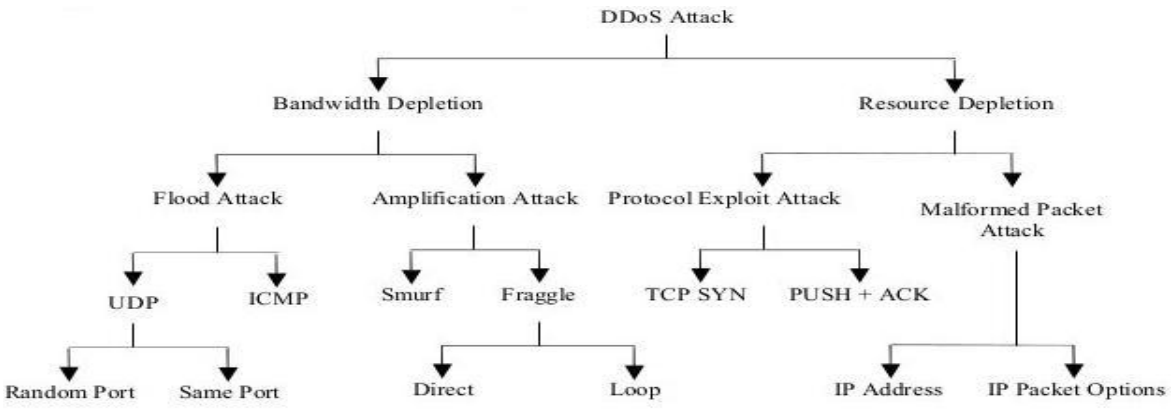

Fig : 3 Techniques of DDoS

Fig:3. 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 primary victim. A resource depletion attack is an attack that is designed to tie up the resources of a victim system making the victim unable to process legitimate requests for service.

3.1 Bandwidth Depletion Attacks

Bandwidth depletion attacks can be characterized as flood attacks and amplification attacks.

Flood Attacks.

A flood attack involves zombies sending a large number of traffic to a victim system, to congest the victim system's network bandwidth with IP traffic. The victim system slows down, crashes, or suffers from saturated network bandwidth, preventing access by legitimate users. Flood attacks have been launched using both UDP (User Datagram Protocol) and ICMP (Internet Control Message Protocol) packets. In a UDP Flood attack, a large number of UDP packets are sent to either random or specified ports on the victim system. The victim system tries to process the incoming data to determine which applications have requested data. If the victim system is not running any applications on the targeted port, it'll send out an ICMP packet to the sending system indicating a destination port unreachable message [5] . Often, the attacking DDoS tool will also spoof the source IP address of the attacking packets. This helps hide the identity of the secondary victims since return packets from the victim system are not sent back to the zombies, but to the spoofed addresses. UDP flood attacks may also fill the bandwidth of connections located around the victim system. This often impacts systems located near the victim. An ICMP flood attack occurs when the zombies send large volumes of ICMP_ECHO_REPLY packets (ping) to the victim system. These packets signal the victim system to reply and the combination of traffic saturates the bandwidth of the victim's network connection [5] . During this attack, the source IP address of the ICMP packet may also be spoofed.

Amplification Attacks.

An amplification attack involves the attacker or the zombies sending messages to a broadcast IP address, using this to cause all systems in the subnet reached by the broadcast address to send a reply to the victim system. The broadcast IP address feature is found on most routers; when a sending system specifies a broadcast IP address as the destination address, the routers replicate the packet and send it to all the IP addresses within the broadcast address range. In this attack, the broadcast IP address is used to amplify and reflect the attack traffic, and thus reduce the victim system's bandwidth.The attacker can send the broadcast message directly, or use the agents to send the broadcast message to increase the volume of attacking traffic. If the attacker decides to send the broadcast message directly, this attack provides the attacker with the ability to use the systems within the broadcast network as zombies without needing to infiltrate them or install any agent software.

A DDoS Smurf attack is an example of an amplification attack where the attacker sends packets to a network amplifier (a system supporting broadcast addressing), with the return address spoofed to the victim's IP address. The attacking packets are typically ICMP ECHO REQUESTs, which are packets (similar to a ping) that request the receiver to generate an ICMP ECHO REPLY packet [6] . The amplifier sends the ICMP ECHO REQUEST packets to all of the systems within the broadcast address range, and each of these systems will return an ICMP ECHO REPLY to the target victim's IP address [7] . This type of attack amplifies the original packet tens or hundreds of times.

Another example is the DDoS Fraggle attack, where the attacker sends packets to a network amplifier, using UDP ECHO packets [8] . There is a variation of the Fraggle attack where the UDP ECHO packets are sent to the port that supports character generation with the return address spoofed to the victim's echo service (echo, port 7 in Unix systems) creating an infinite loop [6] . The UDP Fraggle packet will target the character generator in the systems reached by the broadcast address. These systems each generate a character to send to the echo service in the victim system, which will send an echo packet back to the character generator, and the process repeats. This attack can generate more bad traffic and cause more damage than a Smurf attack.

3.2 Resource Depletion Attacks

DDoS resource depletion attacks involve the attacker sending packets that misuse network protocol communications or are malformed. Network resources are tied up so that none of left for legitimate users.

Protocol Exploit Attacks:

We give two examples, one misusing the TCP SYN (Transfer Control Protocol Synchronize) protocol, and the other misusing the PUSH+ACK protocol. In a DDoS TCP SYN attack, the attacker instructs the zombies to send bogus TCP SYN requests to a victim server in order to tie up the server's processor resources, and hence prevent the server from responding to legitimate requests. The TCP SYN attack exploits the three-way handshake between the sending system and the receiving system by sending large volumes of TCP SYN packets to the victim system with spoofed source IP addresses, so the victim system responds to a non- requesting system with the ACK+SYN. When a large volume of SYN requests are being processed by a server and none of the ACK+SYN responses are returned, the server eventually runs out of processor and memory resources, and is unable to respond to legitimate users.[10]

In a PUSH + ACK attack, the attacking agents send TCP packets with the PUSH and ACK bits set to one. These triggers in the TCP packet header instruct the victim system to unload all data in the TCP buffer (regardless of whether or not the buffer is full) and send an acknowledgement when complete. If this process is repeated with multiple agents, the receiving system cannot process the large volume of incoming packets and the victim system will crash.[10]

Malformed Packet attacks.

A malformed packet attack is an attack where the attacker instructs the zombies to send incorrectly formed IP packets to the victim system in order to crash it.

There are at least two types of malformed packet attacks In an IP address attack, the packet contains the same source and destination IP addresses. This can confuse the operating system of the victim system and can cause the victim system to crash. In an IP packet options attack, a malformed packet may randomize the optional fields within an IP packet and set all quality of service bits to one so that the victim system must use additional processing time to analyze the traffic. If this attack is multiplied, it can exhaust the processing ability of the victim system[9].

4. DDoS COUNTERMEASURES :

One of the effective defense against DDoS identifies the attacked traffic individually than legitimate traffics. Edge routers can be used to mark the source of data packet by using reverse checking mechanism. In case of DDoS attack, a large volume of the data will be coming from certain hosts. If the source IP has been forged, the type of data will be identical for most of the cases. Using TTL(Transistor–transistor logic) or hop counts, data packets can be grouped as trusted or untrusted. To perform this operation, "hardware based checking technology" can be used. This section of the network will use traceback mechanism by using hop count and TTL to test the authenticity of source of data, anomaly of the type of data and classify the source/data as trusted or untrusted. Hardware checking also will maintain a table, which can use certain cache timing, so that traffic from the certain host is not blocked permanently. After certain time, hardware checking will check the incoming data packets from specific host again as that might be a legitimate host machine, which had been compromised because of attackers worm. Updated table of trusted and untrusted hosts should be passed to the next device of the network such as router to send the traffic to the right destination. This device should have the defense mechanism to protect itself from DDoS attack especially for TCP SYN attack. Specific TTL should be assigned traceback operation to verify the source of information. Having hardware checking and filtering technology can work as efficient and cost effective defense mechanism against DDoS attack for any organisation because of less consumption of resources. Proposed hardware-based watermarking technology to detect and prevent DDoS attack will work on following principles:

1) Once packet will reach to the network, the source of the packet will be identified.

2) Traceback mechanism should be used to check the authenticity of source address by using Hop Counts and TTL.

3) If the source cannot be verified, packet will be marked as untrusted and will be dropped without sending it to the internal network.

4) Each packet coming from same untrusted source will be grouped together based on source authenticity

5) If the source is verified, anomaly of the data packets and connection mechanism should be checked against "Next Verification" Step.

6) Any suspicious data packets should be sending to IDS Firewall Proposed System or IPS for in-depth investigation to reduce the rate of false positive or false negative response.

7) Based on known attack type, packet and source should be marked as untrusted and drop the packet on edge of the network.

8) Only "trusted" packets should be marked and passed to the internal network.

Next Verification Steps:

1.) Maintain IP address History(Database)
2.) Store IP address
3.) Store per minute traffic situation and calculate the average of traffic
4.) If traffic of network higher than regular traffic

then check IP address

if its in database => Access granted

else check ip address more than 5 times in history database

if Yes then send it to IDS Firewall Proposed System or IPS for in-depth investigation

else Verified ip and MAC address

if verified => Access Granted

else send it to IDS Firewall Proposed System or IPS for in-depth investigation

5. CONCLUSION

DDoS attacks make a networked system or service unavailable to legitimate users. These attacks are an annoyance at a minimum, or can be seriously damaging if a critical system is a primary victim. Loss of network resources causes economic loss, work delays, and loss of communication between network users. Solutions must be developed to prevent these DDoS attacks.This paper is very beginning of the research to design a cost effective solution for cloud computing environment to prevent DDoS attack. In this early stage

of this research, we tried to identify the variety of DDoS attack and different techniques used by this attack, so that we can design and build the prototype. Hardware based checking and filtering mechanism can provide an additional layer of defense against DDoS attack, which also will consume fewer resources. We will continue this research to present an algorithm, build and test prototype for Hardware based checking and filtering method to prevent the network from DDoS attack.

REFERENCES:

[1] CERT Coordination Center, Denial of Service attacks, Available from <http://www.cert.org/tech_tips/denial_of_ service.html>.

[2] David Karig and Ruby Lee, "Remote Denial of Service Attacks and Countermeasures," Princeton University Department of Electrical Engineering Technical Report CE- L2001-002.

[3] DDoS attacks and defense mechanisms: classification and state-of-the-art by Christos Douligeris , Aikaterini Mitrokotsa http://cys.ewi.tudelft.nl/sites/default/files/comnet.pdf

[4] Kevin J. Houle. "Trends in Denial of Service Attack Technology". CERT Coordination Center, Carnegie Mellon Software Engineering Institute. www.nanog.org/mtg-0110/ppt/houle.ppt

[5] Paul J. Criscuolo. "Distributed Denial of Service Trin00, Tribe Flood Network, Tribe Flood Network 2000, And Stacheldraht CIAC-2319". Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory.

[6] Tech Target by Michael J. Martin Router Expert: Smurf/fraggle attack defense using SACLs
http://searchnetworking.techtarget.com/tip/Router-Expert-Smurf-fraggle-attack-defense-using-SACLs

[7] Federal Computer Incident Response Center (FedCIRC), "Defense Tactics for Distributed Denial of Service Attacks".Washington, DC

[8] Possible fraggel problem http://www-arc.com/sara/cve/Possible_DoS_problem.html

[9]Malformed packet attack
http://www.h3c.com/portal/Products___Solutions/Technology/Security_and_VPN/Technology_White_Paper/20080 4/604013_57_0.htm

[10] Protocol Exploit Attack http://www.cs.unc.edu/~jeffay/courses/nidsS05/slides/5-Protocol-Attacks.pdf

[11] Cisco Systems, Characterising and tracing packet flood using cisco router.

[12] Wikipedia,org