CSCanada
Advances in Natural Science
Vol. 4, No. 2, 2011, pp. 15-17
DOI:10.3968/j.ans.1715787020110402.668

ISSN 1715-7862 [PRINT]
ISSN 1715-7870 [ONLINE]
www.cscanada.net
www.cscanada.org

Distributed Denial of Service Attack Principles and Defense Mechanisms

ZHENG Ying[1,*]

[1]Editorial Department of Journal, Inner Mongolia University for Nationalities, Tongliao, 028043, China
[*]Corresponding author.
Email: mindaxuebao@163.com

Received 30 September 2011; accepted 17 November 2011

Abstract
In recent years, distributed denial of service (DDoS) attacks has brought a grave threat to corporate security and the threats are increasing continuously. The mode and tools of DDoS attacks have become more and more complex and effective and difficult to trace to source, while current defense technology is still not enough to defeat large-scale attacks. The article analyzes the characteristics and types of DDoS attacks in details and discusses the way that attackers control a large number of hosts. Finally control strategies for DDoS attacks are put forward.

Key words: DDoS; Principle; Defense mechanisms; Classification

ZHENG Ying (2011). Distributed Denial of Service Attack Principles and Defense Mechanisms. *Advances in Natural Science, 4*(2), 15-17. Available from: URL: http://www.cscanada.net/index.php/ans/article/view/j.ans.1715787020110402.668
DOI: http://dx.doi.org/10.3968/j.ans.1715787020110402.668.

INTRODUCTION
Distributed denial of service (DDoS) attacks have brought a grave threat to corporate security and the threats are increasing continuously (LI Zhanxin, 2011; Wang Yan, 2011; HU Zun-mei, 2010). A survey shows that some large electronic business companies, such as Amazon, Hotmail and some small ISP are subjected to different degree's DDoS attacks. DDoS attacks send a large number of useless data packets to target server, network even terminal users through lots of controlled hosts so that legal users cannot access to the network normally. In recent years, the mode and tools of DDoS attacks have become more and more complex and effective and difficult to trace to source, while current defense technology is still not enough to defeat large-scale attacks. The article analyzes the characteristics and types of DDoS attacks in details and discusses the way that attackers control a large number of hosts. Finally control strategies for DDoS attacks are put forward.

1. THE PRINCIPLE OF DISTRIBUTED DENIAL OF SERVICE ATTACKS

1.1 The Definition of Distributed Denial of Service Attacks
Denial of service (DoS) means to prevent normal usage service of legal users. When the attacks are only from one host or network node, they are DoS attacks. Distributed denial of service (DDoS) attacks

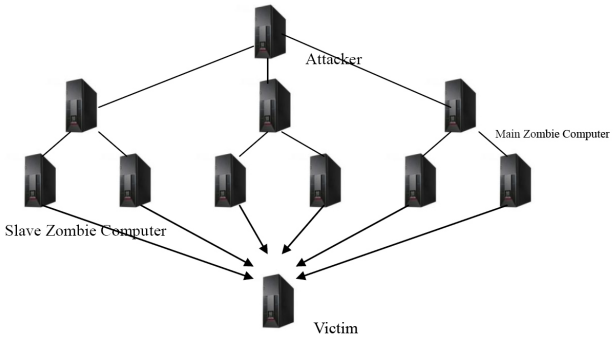

Figure 1
DDoS Attacks Model

brought severer threats(SUN Chang-hua, LIU Bin, 2009). In distributed denial of service (DDoS) attacks, an

attacker controls a great number of hosts to attack targets, leading that legal users cannot access network service normally and resulting in the breaks-down of server(LI Yi-bing,HUANG Xu,No.6,2009; ZENG Wen-quan,XIANG You-jun,SHANG Min,No.7,2009). Shown in Figure 1.

1.2 The Classification of Distributed Denial of Service Attack

Distributed denial of service (DDoS) attacks consumes the resource of target host so that they cannot provide normal service(Cheng Jieren,Yin Jianping,Liu Yun,Cai Zhiping,Li Min,No.8,2009; Zhouenfeng,No.8,2009). One method to classify DDoS attacks is carried out according to the resource it consumes. Generally, the resource that is consumed includes inner resource of hosts of attacked target system and its network transmutability.

1.2.1 Classify According to the Type of the Resource that is Consumed

(1) An example of inner resource attack

An example of inner resource attack is distributed SYN flood attack. The procedure of attacks is below:

a. Attacker controls a great number of hosts on internet and instructs them to contact with target Web server.

b. The host controlled sends TCP/IP SYN packets, and target hosts will receive a lot of information packets with wrong IP addresses.

c. Each SYN packet will set up a TCP link. For each of this kind of packet, Web server will respond to a SYN/ACK packet and then set up a TCP link for the false IP address. Web server will maintain a data structure for each SYN request until it receives responses. But for a great number of requests, Web server will be unable to deal with, leading that the links of legal users are rejected. TCP data structure is a kind of common inner resource and here is given another example of inner resource.

The procedure is below:

a. In many systems, limited data structures are used for saving process information(process marks, items of process table, process slots and so on). An invader consumes these data structures through compiling and copying his owns program or scripts.

b. The invader can also attack through consuming disk space, including producing a great deal of email information; intentionally generating a lot or errors of necessary logins; depositing files in anonymous FTP or network sharing.

(2) An example that consumes network transmission resource

A distributed ICMP attack belongs to the case of attack that consumes network transmission resource and the procedure is below:

a. The attacker controls a great number of hosts on Internet and instructs them to send ICMP ECHO packets(IP addresses in the packet are false) to a set of hosts that are taken as gangplanks.

b. When the nodes as gangplanks receive those cheating requests, they send response packets to target websites.

c. The routers of target hosts receive a lot of packets sent by gangplanks websites so that routers are unable to deal with legal requests.

1.2.2 Direct DDoS Attacks and Gangplank DDoS Attacks

Another method to classify DDoS attacks is to divide them into direct DDoS attacks and gangplank DDoS attacks.

(1) Direct DDoS attacks

In direct DDoS attacks, attackers are able to implant corpse software into a great number of hosts on Internet. Generally, DDoS attacks include two-class corpse computer: main corpse and sub-corpse. Two kinds of corpse computers are infected by malicious codes. Attackers control main corpse and corresponding main corpse controls sub-corpse. Adopting two-class corpse structure makes it more difficult to trace the source of attacks and thus provide a more flexible network.

(2) Gangplank DDoS attacks

In gangplank DDoS attacks, a layer of computers are increased. In this type of attacks, sub-corpse structures corresponding response packets. The IP addresses of target hosts are filled in the original IP address in IP packets and then these packets are sent to the hosts without being infected as gangplanks. And then the hosts send response packets to target hosts. Gangplank DDoS attacks brings larger flows and thus its harm is stronger. In addition, tracing attackers and filtering attacks packets are also more difficult because the attacks are brought by a lot of hosts without being infected on internet.

1.3 The Method of DDoS Attacks

In DDoS attacks, the step is that the attacker infects mass hosts and installs corpse software on them. Finally the hosts execute attacking task. The essence of attacks is below:

a. The software that can execute DDoS attacks. The software has to be able to operate in a lot of hosts and hide itself, as well as contact with attackers or bring expected attacks to targets through certain time triggered mechanism.

b. A lot of hosts have bugs. Attackers should be clear that a lot of hosts have bugs. The hosts' administers or individual users do not pitch the system correspondingly so that attackers can install corpse software on them.

c. The strategy to search the host existing bugs, for example, scanning.

In the process of scanning, attackers find the host that has bugs and infect them firstly, and then install corpse software on it and copy the process of scanning until that the large distributed network that is composed of infected computers is set up.

Here are some strategies of scanning below:

a. Random: Each host adopts different seeds to detect

random addresses in the range of IP addresses. The technology will produce very large flows and thus great damages have been caused before practical attacks.

b. Attack list: Attackers compile a list of hosts that may have bugs firstly. In order to avoid being detected, it may be a long and slow course. Once the list is compiled, attackers begin to infect the hosts. Each infected host can scan a part of the host in the list. The strategy makes the time of scanning short and the difficulty in detecting infection increased.

c. Local anatomy: The mode makes use of the information in each infected host to scan more hosts.

d. LAN Sub-net: If the host protected by firewall is infected, it searches target in its local area network (LAN) and uses the address structure inside sub-net to search other hosts.

2. DISTRIBUTED DENIAL OF SERVICE ATTACK PREVENTION AND TREATMENT STRATEGIES

Generally, there are three strategies for dealing with DDoS attacks(Chang R,October,2002) as follows:

a. Attacks pre-warning and first-mover mechanism (before attacks): The mechanism makes it can endure the attacks and the requests of legal users are not rejected. The technologies include adopting compulsory strategies for the consumption of resource and providing reserve resource according to the demand possibly. In addition, preventive mechanism improves systems and network protocols so that the possibility of subjecting to DDoS attacks reduces.

b. Attacks detection and filter mechanism(in attacks): The mechanism makes it responses to the attacks as soon as possible through attacks detection, which reduces the influence of attacks on targets to the limit. Detection includes searching suspicious deeds. Response includes filtering certain possible attacks packets.

c. The traces and recognition of tracks sources(in attacks and after attacks): Attempting to recognize attacks sources is the first step in order to prevent attacks. Generally, the attacks sources cannot be found soon, but this reduces the attacks that appear now. Coping with the challenges brought by DDoS attacks is a hard way, but corresponding control strategies develop immediately.

REFERENCES

[1] Chang R. (2002, October). Defending Against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial. *IEEE Communications Magazine.*

[2] CHENG Jieren, YIN Jianping, LIU Yun, CAI Zhiping, & LI Min (2009). Detecting Distributed Denial of Service Attack Based on Address Correlation Value. *Journal of Computer Research and Development,* (8), 1334-1340.

[3] HU Zunmei (2010). Summary of Defense Mechanism on DDoS Attack. *Computer Security,* (4), 64-65.

[4] LI Yibing, HUANG Xu (2009). New Improved Compositive DDoS Defence System. *Application Research of Computers,* (6), 2119-2121.

[5] LI Zhanxin (2011). Attacks Principle and Prevention Tactics of Distributed Denial of Service. *Computer Programming Skills & Maintenance,* (16), 132-134.

[6] WANG Yan (2011). Performance Analysis on Techniques of Tracing Network Attacks. *Computer Applications and Software*, (2), 294-297.

[7] SUN Changhua, LIU Bin (2009). Survey on New Solutions Against Distributed Denial of Service Attacks. *Acta Electronica Sinica,* (7), 1562-1570.

[8] ZENG Wenquan, XIANG Youjun, & SHANG Min (2009). Analysis of Principle and Defense of DDoS Attacks. *Computer Technology and Development,* (7), 156-158,162.

[9] ZHOU Enfeng (2009). Distributed Denial of Service Attack Principles and Prevention. *China Computer & Communication,* (8), 64.

