Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Denial of Service Attacks

Shenam Chugh, Dr. Kamal Dhanda
Department of CSE, BRCM Bahal,
Bhiwani, Haryana, India

Abstract: This paper is a review on the problem of denial-of-service (DoS) attacks and proposed ways to deal with it. Broadcast authentication is an important application in sensor networks.Public Key Cryptography (PKC) is desirable for this application,but due to the resource constraints on sensor nodes, these operations are expensive, which means sensor networks using PKC are susceptible to Denial of Service (DoS) attacks: attackers keep broadcasting bogus messages, which will incur extra costs, thus exhaust the energy of the honest nodes. In addition, the long time to verify each message using PKC increases the response time of the nodes; it is impractical for the nodes to validate each incoming message before forwarding it.We describe the nature of the problem and look for its root causes,further presenting brief insights and suggested approaches for defending against DoS.

Key Words: Denial of Service, Distributed Denial of Service, Network Traffic, Internet Security, Wireless Security

I. INTRODUCTION

To secure computer systems it is important to consider the concept of CIA: confidentiality, integrity and availability. With respect to availability, hackers continue to focus on preventing access to online services and systems by crashing a service through exploitation or by flooding services to the point that the resource is no longer accessible. These types of denial-of-service or DoS attacks can come directly from one IP address or from a multitude of computers located in disparate locations, known as Denial of Service (DoS).

A denial of service attack on a network could take one of three possible forms. A malicious party (a.k.a.the attacker) could cause the network not to transmit messages it should be sending in order to offer service to a subset or all of its clients. On the other end of the spectrum, the network could be caused to send messages, which it should not be sending. By far the most common form of DoS in today's networks is causing excessive bogus traffic (a.k.a. flooding the network) in the direction of a particular server, which in the end will prevent legitimate users from getting the service they could otherwise be receiving from that server.

A simple example of denial of service attack is the popular SYN attack on the TCP protocol. A client sends a request (SYN) to a server announcing its intention to start a conversation. The server responds with an acknowledgement (SYN ACK), accepting the establishment of a connection to the client and simultaneously reserving an entry for the pending connection in its connection queue. Now it is the client's turn to acknowledge the start of the communication by sending its (SYN ACK ACK) packet. A malicious client may never do that, as a result the server ends up with its connection queue entry tied up (and unused) for a significant amount of time (at least as long as the timeout), before it can be released. If one imagines the above scenario repeating over multiple (almost) simultaneous client requests, it is easy to see how the server could be tricked into initiating bogus "communication" with one of more malicious client(s). Since the maximum processing power of a typical 100 MIPS class server is on the order of 1000 to 2000 connections per second [SPEC96] and the minimum standard server TCP connection queue is 2048 slots [DEC96], it becomes clear that overwhelming even a powerful server is within the capabilities of even a very small number of conspiring malicious clients.

II. TYPES OF DOS ATTACK

Before classification of DoS attacks, we describe a typical DoS attack scenario. Then we introduce why it is so prevalent, and its intrinsic reasons why it is so easy to launch. Figure (1) shows a hierarchical model of a DoS attack. DoS attack divide into 2 types. One is bandwidth depletion. This method is to congest the network, massive use of the bandwidth then lead the network breakdown. The other type is resource depletion. Attacker depletes the key resources such as CPU, memory and so on. Then break the server [1]. The attack usually starts from numerous sources to aim at a single target. Multiple target attacks are less common; however, there is the possibility for attackers to launch such type of attack Spoofed, altered, or replayed routing information

2.1 SYN flood attack

Any system providing TCP-based network services is potentially subject to this attack. The attackers use half-open connections to cause the server exhaust its resource to keep the information describing all pending connections. The result would be system crash or system In operative [8].

2.2 TCP Reset Attack

TCP reset also utilize the characteristics of TCP protocol. By listening the TCP connections to the victim, the attacker sends a fake TCP RESET packet to the victim. Then it causes the victim to in advertently terminate its TCP connection [2].

2.3 ICMP attack

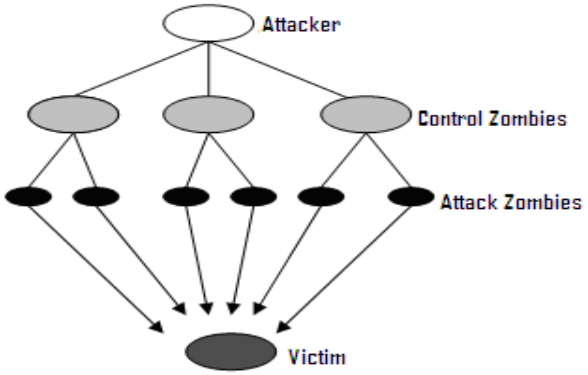
Smurf attack sends forged ICMP echo request packets to IP broadcast addresses. These attacks lead large amounts of ICMP echo reply packets being sent from an intermediary site to a victim,accordingly cause network congestion or outages [CER98]. ICMP datagram can also be used to start an attack via ping. Attackers use the ping Command to construct oversized ICMP datagram to launch the attack [6].

2.4 UDP storm attack

This kind of attack can not only impair the hosts. Services, but also congest or slow down the prevailing network. When a connection is established between two UDP services, each of which produces a very huge number of packets, thus cause an attack.

2.5 DNS request attack

In this attack scenario, the attack sends a large number of UDP-based DNS requests to a name server using a spoofed source IP address. Then the name server, acting as an intermediate party in the attack, responds by sending back to the spoofed IP address as the victim destination.
Because of the amplification effect of DNS response, it can cause serious bandwidth attack [9].



2.6 CGI request attack

By simply sending multiple CGI request to the target server, the attacker consumes the CPU resource of the victim. Then the server is forced to terminate its services.

2.7 Mail bomb attack

A mail bomb is the sending of a enormous amount of e-mail to a specific person or system. A huge amount of mail may simply fill up the recipient's disk space on the server or, in some cases, may be too much for a server to handle and may cause the server to stop working. This attack is also a kind of flood attack [3].

2.8 ARP storm attack

During a DoS attack, the ARP request volume can become very massive, and then the victim system can be negatively affected

2.9 Algorithmic complexity attack

It's a class of low-bandwidth DoS attacks that exploit algorithmic deficiencies in the worst case performance of algorithms used in many mainstream applications. For example, both binary trees and hash tables with carefully chosen input can be the attack targets to consume system resources greatly [3].

2.10 Spam Attack

This type of attack is used for targeting the various mail services of corporate as well as public users. DoS attack through spam has increased and disturbed the mail services of various organizations. Spam penetrate through all the filters to create DoS attacks, which causes serious trouble to users and the data. But these mail services are frequent target of hackers and spammers.[7]

III. CHARACTERISTICS OF DISTRIBUTED DENIAL OF SERVICE ATTACKS

A denial of service attack is characterized by an explicit attempt by an attacker to prevent legitimate users of a service from using the desired resources. Examples of denial of service attacks include :

- attempts to "flood" a network, thereby preventing legitimate network traffic
- attempts to disrupt connections between two machines, there by preventing access to a service
- attempts to prevent a particular individual from accessing a service
- attempts to disrupt service to a specific system or person.

The distributed format adds the "many to one" dimension that makes these attacks more difficult to prevent [12].A distributed denial of service attack is composed of four elements, as shown in Figure 2 [11]. First, it involves a victim, i.e., the target host that has been chosen to receive the brunt of the attack. Second, it involves the presence of the attack daemon agents. These are agent programs that actually conduct the attack on the target victim. Attack daemons are usually deployed in host computers. These daemons affect both the target and the host computers. The task of deploying these attack daemons requires the attacker to gain access and infiltrate the host computers. The third component of a distributed denial of service attack is the control master program. Its task is to coordinate the attack. Finally, there is the real attacker, the mastermind behind the attack. By using a control master program, the real attacker can stay behind the scenes of the attack. The following steps take place during a distributed attack:

1. The real attacker sends an "execute" message to the control master program.
2. The control master program receives the "execute" message and propagates the command to the attack daemons under its control.
3. Upon receiving the attack command, the attack daemons begin the attack on the victim.

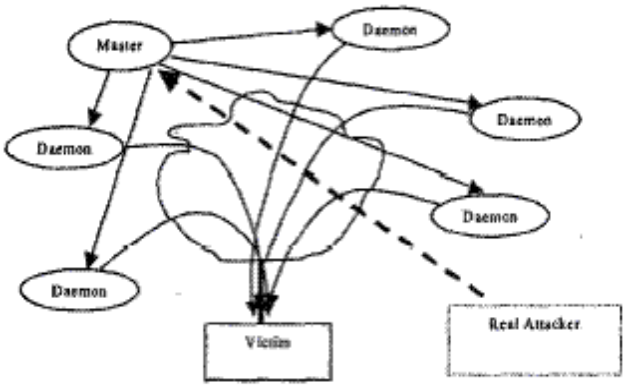


Figure 2: The four components of a distributed denial of service attack: a real attacker, a control master program, attack daemons and the victim [11].

Although it seems that the real attacker has little to do but sends out the "execute" command, he/she actually has to plan the execution of a successful distributed denial of service attack. The attacker must infiltrate all the host computers and networks where the daemon attackers are to be deployed. The attacker must study the target's network topology and search for bottlenecks and vulnerabilities that can be exploited during the attack. Because of the use of attack daemons and control master programs, the real attacker is not directly involved during the attack, which makes it difficult to trace who spawned the attack.

IV. CONCLUSIONS

Efficiency and scalability are the key requirements in design of defence against DoS attacks. In this paper, we discussed denial of service attacks on the Internet. We described how attacks are conducted, we reviewed some well known denial of service attacks. One great advantage of the development of DoS attack and defence classifications is that effective communication and cooperation between researchers can be achieved so that additional weaknesses of the DoS field can be identified DoS attacks are not only a serious threat for wired networks but also for wireless infrastructures.

REFRENCES

[1] Liang Hu, Xiaoming Bi, "Research of DDoS Attack Mechanism and Its Defense Frame,"Computer Research and Development (ICCRD), 3rd International Conference, pp. 440–442, March 2011.

[2] Robert Vamosi, "Study: DDoS attacks threaten ISP infrastructure," Online at http://news.cnet.com/8301-1009_3-10093699-83.html, CNET News, Nov. 2008.

[3] Elinor Mills, "Radio Free Europe DDOS attack latest by hactivists," Online at http://news.cnet.com/8301-10784_3-9933746-7.html, CNET News, May. 2008.

[4] Christos Douligeris and Aikaterini Mitrokotsa, "DDoS Attacks And Defence mechanisms: A Classification," in Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology, (ISSPIT'03), pp. 190-193, Dec 2003.

[5] IEEE Communications Magazine, pp. 42-51, Oct. 2002 Rocky K. C. Chang," Defending against Flooding-based Distributed Denial-of-service Attacks: A Tutorial,".

[6] Internet World Stats, Internet User Statistics – The Big Picture: World Internet Users andPopulation Stats, http://www.internetworldstats.com/stats.htm

[7] Dhinaharan Nagamalai, Cynthia Dhinakaran, Jae Kwang Lee. "Multi Layer Approach to Defend DDoS Attacks Caused by Spam". In aaXiv.org (Cornell university Library),arXiv: 1010.1583v1 [cs.CR]

[8] S. M. Khattab, C. Sangpachatanaruk, R. Melhem, D. Mosse, and T. Znati, "Proactive Server Roaming for Mitigating Denial-of-Service Attacks," in Proceedings of the 1st International Conference on International Technology: Research and Education (ITRE'03), pp. 286-290, Aug.2003.

[9] A. Yaar, A. Perrig, and D. Song, "PI: A path identification mechanism to defend against DDoS attacks," in proceedings of the IEEE symposium on Security and Privacy, pp. 93-109, May 2003.

[10] S. Bellovin, "Security problems in the TCP/IP protocol suite," *Comput. Commun. Rev.,* vol. 19, no. 2, pp. 32-48, Apr. 1989.

[11] S. Bellovin, "Distributed denial of service attacks," Feb. 2000, http://www.research.att.com/~smb/talks.

[12] B. Martin, "Have script, will destroy (lessons in DoS)," Feb. 2000, http://www.attrition.org.

