OVERVIEW ON DISTRIBUTED DENIAL-OF- SERVICE ATTACKS AND PREVENTION

Dr.S.VENNILA
Assistant Professor in Computer Application
St.Ann's college of Arts and Science, Tindivanam

Abstract

Distributed Denial-of-service (DDoS) attack is one of the most dan-gerous threats that could cause devastating effects on the Internet. DDoS mainly started in 1998 but the influence of it was realized by the people only when the big organizations and corporations were hit by DDoS attacks in July 1999. Since then several DDoS attack tools such as Trinoo, Shaft, Tribe flood net- work (TFN), Tribe flood network 2000 (TFN2K) and Stacheldraht are identified and analyzed. All these tools could launch DDoS attacks from thousands of compromised host and take down virtually any connection, any network on the Internet by just a few command keystrokes. This survey paper deals with the introduction, history, DDoS attack strategy, and classification of various attack and Prevention mechanisms has been pointed out.

Introduction

A Denial of Service attack is an attempt by a person or a group of persons to cripple an online service. This can have serious consequences, especially for companies like Amazon and eBay which rely on their online availability to do business. In the not so distant past there have been some large scale attacks targeting high profile internet sites. Consequently, there are currently a lot of efforts being made to come up with mechanisms to detect and mitigate such attacks.

Even though the first denial of service attacks did not take place a long time ago (tools that automate setting up of an attack network and launching of attacks, started appearing in 1998), there are a multitude of denial of service attacks that have been used. Broadly speaking the attacks can be of three forms. a) Attacks exploiting some vulnerability or implementation bug in the software implementation of a service to bring that down .b) Attacks that use up all the available resources at the target machine. c) Attacks that consume all the bandwidth available to the victim machine.

The third type of attacks are called **bandwidth attacks**. A distributed framework becomes especially suited for such attacks as a reasonable amount of data directed from a number of hosts can generate a lot of traffic at and near the target machine, clogging all the routes to the victim. Protection against such large scale distributed bandwidth attacks is one of the most difficult (and urgent) problem to address in today's internet. CERT reports bandwidth attacks as increasingly being the most common form of Denial of Service attacks seen in the internet today.

HistoryandTrendsinDDoSattacks.

The DDoS attacks gained very widespread notoriety and media exposure with the three days of DoS attacks(Feb 7-11, 2000) that were launched against major internet sites like CNN, Yahoo, EBay and Datek. Multiple attack tools like Trinoo, TFN, StachleDraht, TFN2K were used in these attacks. Ironically, these attacks came just a day after Steve Bellovin's talk on Distributed Denial of Service at NANOG (North American Network Operator's Group) in San Jose. But, Denial of Service attacks had been observed, studied and some attack tools like Trinooand TFN ,TFN2K,Smurf Attacks .

The sophistication of the DDoS attack tools has kept on improving with time. Therefore a historical study of DDoS attacks also gives a good overview of the various techniques that are used in organize such attacks. This section starts off with an explanation of the steps involved in DDoS attack.

DDoS attack, three steps are needed: Scanning, Propagation and Communication.

Scanning is the first step to exploit any system. The attacker first recruits the machines that have some Affects. Earlier this process was done manually by the attacker but now this process is automated. Some scanning strategies such as hit list scanning, topological scanning, permutation scanning, and local subnet scanning are popular or potential in deployment of DDoS attacks . Attacker uses these techniques to continuously scan the vulnerable machines over the Internet and installs malicious scripts into them. So these machines become capable of recruiting other slaves or zombies under them too.

Propagation: While scanning deals with just looking for vulnerable machines, propagation deals with recruiting further machines with the help of already compro- mised machines which can be used further to generate a stream of packets towards the victim` s machine. Central source propagation model, back-chaining model and auto-nomous model are three main models of propagation .

Communication: The communication channel is important for coordinating an attack. Either Agent-Handler model or IRC model can be used to communicate with each other. In Agent-Handler Modal communication can be done by using TCP/ICMP/UDP protocol between attacker to handler, handler to agent and vice versa. In this model the communicators know each other` s identity. Internet Relay Chat (IRC) is a multi-user, on-line chatting system. In IRC (Internet Relay Chat) Model, the communicators cannot communicate directly so tracebacking is not easy that make it most widely used model by the attackers over a network.

DDoS Attack Strategy

Launching DDoS attack involves four components: attacker, control masters (or han-dlers), agents (or slaves or zombies), victim (or target machine). Attacker first scans

millions of machines over the Internet for finding vulnerable machines whose security can be exploited easily. These machines are known as masters or handlers as these are directly under the control of attacker. The process of recruiting handlers is completely auto-mated and is done through continuous scanning of remote machines looking for any security loopholes. The attacker installs malicious codes into these infected machines which then become capable of deploying further infected machines.

The machines deployed by handlers are directly under their control and are known as slaves or zombies. Attacker indirectly controls these machines through handlers. These handlers and zombies, on the signal of attacker are used to start a coordinated attack on target machine. This makes the target machine incapable of communicating or utilizing any of its resources. Attacker often uses IP spoofing in handlers and zombies to hide the identity of these machines. This leaves future scope for attacker of using the same machines for creating DDoS attack.

Classification of DDoS Attack

We can classify DDoS attacks into two broad categories: flooding attacks and logical attacks . Flooding attacks creates avalanche of transmitting packets at the victim side which makes the target machine incapable of handling request from the legiti- mate users.

Flooding attacksThe attacker keeps on sending request packets to the server at a particular rate. Due to increase in attack packets, the legitimate users decrease their flow of packets as per network Congestion control mechanism. Once the total request rate from the server becomes greater than the service rate of the server, the request packets starts getting buffered in the server and after some time the re-rqests start dropping down. Finally, the time comes when whole of the bandwidth is exhausted by the attack packets only and the legitimate users are denied of the services, thus creating successful DDoS attack. In Logical or software attack, a small number of malformed packets are de-signed to exploit known software bugs on the target system. These attacks are relatively easy to counter either through the installation of software patches that eliminate the vulnerabilities or by adding specialized firewall rules to filter out malformed packets before they reach the target system

Types of flooding Attack

i). SYN flooding attack: A normal TCP connection involves 3-way handshaking. In case of attack, the attacker uses spoofed IP addresses to send requests to a server. The server responds by sending the SYN/ACK signal waiting for the ACK signal from its client. But this time no reply comes since the IP is spoofed and the real client is unaware of the ACK signal that the server is expecting. This leaves the half open connections on the server side thus consuming its resources. Therefore, creating thou- sands and thousands of requests like this can force the server to crash or hang.

ii). ICMP attack: An attacker sends forged ICMP echo packets to broadcast addresses of vulnerable networks. All the systems on this network reply to the victim with ICMP ECHO replies. This rapidly exhausts the bandwidth available to the target, effectively denying its services to legitimate users.

iii). UDP Flood Attack: A UDP flood attack is possible when an attacker sends a UDP packet to a random port on the victim system. The victim system will look for the application waiting on that port. When it realizes that there is no application that is waiting on the port, it generates an ICMP packet of destination unreachable to the forged source address. If flood of UDP packets are send to the victim machine, the system will surely go down .

Types of Logic Attack

i) Ping of Death: It's the use of ping command to exploit the fact that the maximum packet size that TCP/IP allows for being transmitted over the Internet is restricted to65,536 octets. In this attack, the target system is pinged with a data packet that ex- ceeds the maximum bytes allowed by TCP/IP. A simple command

C:\>ping 66000 hostname can force the system to hang or crash. Nowadays our host systems are safe from this type of attack because these attacks were prevalent in UNIX systems [2].

ii) Teardrop Attack: Whenever a packet is send over the Internet, it is broken down into fragments at the source system and reassembled at the destination system. An attacker sends two fragments that cannot be reassembled properly making use of a bug in the TCP/IP fragmentation re-assembly code of various operating systems by manipulating the off-set value of packet and cause re-boot or halt the victim system.

iii) Land Attack: An attacker sends a forged packet with the same source and destination IP address. Whenever victim system replies to that packet it actually sends that packet to itself, has creating an infinite loop between the target system and target system itself thus causing the system to crash or re-boot.

DDoS Prevention Mechanisms

DDoS Attack Prevention: Attack prevention methods try to stop all well known signature based and broadcast based DDoS attacks from being launched in the first place or edge routers, keeps all the machines over Internet up to date with patches and fix security holes. Signature of the packets is matched with the existing database consisting of known attack patterns at each edge router. To prevent the DDoS attack against target machine we have the following approaches:-

i) Filtering all packets entering and leaving the network protects the network from attacks conducted from neighboring networks, and prevents the network itself from being an unaware attacker. This measure requires installing ingress and egress packet filters on all routers. It is used to filter spoofed IP address but approaches to prevent it needs global implementation that is not practical.

ii) Firewall can allow or deny protocols, ports or IP addresses but some complex attack like on port 80 cannot be handled by it because it is unable to distinguish between valid traffic and DDoS attack traffic. Only those attacks can be identified whose signatures are already there in the database. A slight variation from the original attack pattern can leave the attack undetected. Also new attacks cannot be detected.

iii) Service Level Agreements (SLA). SLA helps to prevent DoS and DDoS attacks. Standardized SLA, which is the only legal agreement between a client and the service provider for availability, confidentiality and trust. An SLA can take care of the following: (1) privileged user access, that assures the customer outsourced sensitive data do not fall into malicious hands; (2) regulatory compliance, that holds the customer ultimately responsible for his own data, and subjects the service provider to external audits and security certifications; (3) data location, that is a commitment to comply to the local jurisdiction and to store and process data in specific jurisdictions only and (4) data segregation: data must be properly encrypted to avoid leakages between users sharing the same environment. The authors also provide a list of questions that SLA must answer.

iv.DDoSAttack Mitigation Architecture: DaMask. Wang et al. proposea DDoS attack mitigation architecture. The Software-Defined Networking (SDN) is an approach that allows network administrators to manage network services by way of abstraction of lower-level functionality. The authors find that the SDN and Cloud Computing can enhance the DDoS attack defense. The DaMask architecture has three layers: network switches, network controllers and network applications. There are two separate modules: (1) DaMask-D, a network attack detection system, and (2) DaMask-M, an attack reaction module. DaMask-D already has an efficient attack detection algorithm with a very low overhead. DaMask-M defines three basic operations: forward, drop and modify the packet. Those operations are implemented as a set of APIs. Consequently, the defenders can customize the countermeasures.

Reference

1. Leiner, B.M., Cerf, V.G.: A Brief History of the Internet, http://www.isoc.org

2. Sachdeva, M., Singh, G., Kumar, K., Singh, K.: DDoS Incidents and their Impact: A Review. The International Arab Journal of Information Technology 7(1), 14–20 (2010)

3. Xiang, Y., Zhou, W., Chowdhury, M.: A Survey of Active and Passive Defense Mechanisms against DDoS Attacks. Technical Report, TR C04/02, School of Information Technology, Deakin University, Australia (2004)

4. Houle, K.J., Weaver, G.M.: Trends in Denial of Service Attack Technology, CERT (October 2001), http://www.cert.org/archive/pdf/DoS_trends.pdf

5. Dittrich, D.: The DoS Project's Trinoo Distributed Denial of Service attack tool, University of Washington (October 21, 1999), http://staff.washington.edu/dittrich/misc/trinoo.analysis.txt

6. Molsa, J.: Mitigating denial of service attacks: A tutorial. Journal of Computer Securi- ty 13, 807–837 (2005) . CERT, CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks (Sep-tember 1996)

7. Paxson, V.: Bro: A System for Detecting Network Intruders in Real-Time. InternationalJournal of Computer and Telecommunication Networking 31(24), 2435–2463 (1999)

8. Stone, R.: CenterTrack: An IP Overlay Network for Tracking DoS Floods. In: 9th UsenixSecurity Symposium, pp. 199–212 (August 2000)

9. Burch, H., Cheswick, B.: Tracing Anonymous Packets to Their Approximate Source. In: Proceedings of the 14th Systems Administration Conference (LISA 2000), New Orleans, Louisiana, USA (December 2000)

10. Bellovin, S.M.: ICMP Traceback Messages, Internet Draft, Network Working Group(2000)

11. Mankin, A., Massey, D., Wu, C.-L., Felix Wu, S., Zhang, L.: On Design and Evaluation of Intention-Driven ICMP Traceback. In: Proceedings of Computer Communications and Networks (2001)

12. Wang, B., Schulzrinne, H.: A Denial-of-Service-Resistant IP Traceback Approach. In:3rd New York Metro Area Networking Workshop, NYMAN 2003 (2003)

13. Kumar, K., Joshi, R.C., Singh, K.: An Integrated Approach for Defending against Distributed Denial-of- Service (DDoS) Attacks. In: Proceedings of IRISS-2006, IIT Madras (2006), http://www.cs.iitm.ernet.in/~iriss06/iitr_krishan.pdf

14. trends in Denial of Service Technology . http://www.cert.org/archive/pdf/DoS_trends.pdf

15. Usenix Security Symposium, 2000 talk by Dave Dittrich. ftp://ftp.ddj.comT/technetcast/mp3/tnc-0417-24.mp3 .