RESEARCH ARTICLE OPEN ACCESS

A Survey on Solutions to Distributed Denial of Service Attacks

Badrinath K [*], Mahesh Raj Urs [**], Anand Tilagul [***]
[*] (Dept of Information Science, SJCIT Chickballapur-562101)
[**] (Dept of Information Science, SJCIT Chickballapur-562101)
[***] (Dept of Information Science, SJCIT Chickballapur-562101)

Abstract
Distributed Denial of Service (DDoS) attack is a large-scale, coordinated attack on the availability of services of a victim system or network resource, launched indirectly through many compromised computers on the Internet. Researchers have come up with more and more specific solutions to the DDoS problem. However, existing DDoS attack tools keep being improved and new attack techniques are developed. It is desirable to construct comprehensive DDoS solutions to current and future DDoS attack variants rather than to react with specific countermeasures. In order to assist in this, we conduct a thorough survey on the problem of DDoS. We propose taxonomies of the known and potential DDoS attack techniques and tools. Along with this, we discuss the issues and defend challenges in fighting with these attacks. Based on the new understanding of the problem, we propose classes of solutions to detect, survive and react to the DDoS attacks

I. Introduction

A denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. Typically the targets are high-profile web servers, the attack aiming to cause the hosted web pages to be unavailable on the Internet. Denial of service attack programs, root kits, and network sniffers have been around for a very long time. Yet this point-to-point denial of service attacks can be countered by improved tracking capabilities to shut down the source of the problem. However, with the growth of the Internet, the increasingly large number of vulnerable systems are available to the attackers. Rather than relying on a single server, attackers could now take advantage of some hundred, thousand, even tens of thousands or more victim machines to launch the distributed version of the DoS attack. A distributed denial of service attack (DDoS attack) is a large-scale, coordinated attack on the availability of services of a victim system or network resource, launched indirectly through many compromised computers on the Internet [1].

There have been a number of proposals and solutions to the DDoS attacks. However there is still no comprehensive solution which can protect against all known forms of DDoS attacks. This paper tries to analyze and classify the current solutions to the DDoS attack. By examining the pros and cons of each solution, we can know about the effectiveness of the solutions.

In Section 2, we describe the steps it takes to launch the DDoS attack and examine the attack strategies. In Section we also discuss the current trend in DDoS attack. In Section 4, we propose classes of DDoS countermeasures and analyze the desirability of those solution. Finally, We conclude the paper in Section 5.

II. Overview of DDoS Attacks

2.1 Attack Strategies

DDoS attacks can be divided into two categories: bandwidth Attack and resource attack. A bandwidth attack simply try to generatepackets to flood the victim's network so that the legitimate requests cannot go to the victim machine. A resource attack aims to send packets that misuse network protocol or malformed packets to tie up network resources so that resources are not available to the legitimate users any more.

2.1.1 Bandwidth Attacks

2.1.1.1 Flood Attack

In a direct attack, zombies flood the victim system directly with IP traffic. The large amount of traffic saturates the victim's network bandwidth so that other legitimate users are not able to access the service or experience severe slow down. Normally in those attacks, the following packets are used.

- TCP floods A stream of TCP packets with various flags set are sent to the victim IP address. The SYN, ACK, and RST flags are commonly used.
- ICMP echo request/reply (e.g., ping floods) A stream of ICMP packets are sent to a victim IP address.
- UDP floods A stream of UDP packets are sent to the victim IP address.

2.1.1.2 Reflected Attack

A reflected denial of service attack involves sending forged requests of some type to a very large number of computers that will reply to the requests. Using Internet protocol spoofing, the source address is set to that of the targeted victim, which means all

the replies will go to (and flood) the target. ICMP Echo Request attacks can be considered one form of reflected attack, as the flooding host(s) send Echo Requests to the broadcast addresses of mis-configured networks, thereby enticing a large number of hosts to send Echo Reply packets to the victim. Some early DDoS programs implemented a distributed form of this attack. Nowadays, DNS attacks using recursive name servers can create an amplification effect similar to the now-aged Smurf attack [2].

2.1.2 Resource Attacks

2.1.2.1 TCP SYN Attack

The TCP SYN attack exploits the three-way handshake between the sender and receiver by sending large amount of TCP SYN requests with spoofed source address. If those half-open connection binds resources on the server or the server software is licensed per-connection, all these resources might be taken up.

2.1.2.2 Malformed Packet Attack

A ping of death (abbreviated "POD") is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A ping is normally 64 bytes in size; many computer systems cannot handle a ping larger than the maximum IP packet size which is 65,535 bytes. Sending a ping of this size often crashes the target computer

.

III. DDoS Attack Trends

There is little change in the nature of the targets of DoS attacks. The Internet community, ranging from individual end-users to the largest organizations, continues to experience DoS attacks. Following are the technology trend of current DDoS attacks:

- **Larger botnet size** There is a steady increase in the ability for intruders to easily deploy large DDoS attack networks. In the race of available consumable resources versus the ability to consume those resources, todays DDoS networks continue to outpace available bandwidth in most cases.
- **Advances in master-zombie communications** Recently, there is an increase in intruder use of Internet Relay Chat (IRC) protocols and networks as the communications backbone for DDoS networks. The use of IRC essentially replaces the function of a handler in older DDoS network models. IRC-based DDoS networks are sometimes referred to as botnets, referring to the concept of bots on IRC networks being softwaredriven participants rather than human participants. The use of IRC networks and protocols makes it more difficult to identify DDoS networks.
- **Base on legitimate traffic** Where packet filtering or rate limiting can be effective to control the impact of some types of DoS attacks, intruders are beginning to more often use legitimate, or expected, protocols and services as the vehicle for packet streams. Doing so makes filtering or rate limiting based on anomalous packets more difficult. In fact, filtering or rate limiting an attack that is using a legitimate and expected type of traffic may in fact complete the intruders task by causing legitimate services to be denied.
- **Less reliance on source address spoofing** Although it is still used, less emphasis is put on source IP address spoofing in DoS attacks. With highly distributed attack sources, that many times cross several autonomous system (AS) boundaries, the number of hosts involved as sources of an attack can be simply overwhelming and very difficult to address in response. Source IP address spoofing simply is not a requirement to obfuscate large numbers of attack sources and enable the attacking party to avoid accountability for the attack.

IV. Taxonomies of DDoS Defense Mechanisms

The DDoS defense mechanisms can be roughly divided into two categories: Survival Mechanisms and Reactive Mechanisms.

4.1 Survival Mechanisms

Survival mechanisms involves increasing the effective resources to such a degree that DDoS effects are limited. This kind of enlargement can be achieved statically by purchase more hardware and use load balance techniques to increase the system capacity, or dynamically by acquiring resources at the time of DDoS attack and replicate the service.

However, the arm race with DDoS attackers still seems to be hard for the victims, as it is easier for attackers to acquire additional thousands of zombies to win the race. Thus this kind of approach cannot give a complete solution to DDoS.

4.2 Reactive Mechanisms

Reactive mechanisms try to detect the occurrence of the attack and react to that either by controlling attack streams, or by attempting to locate agent machines and invoking human action. There has been numerous proposals and partial solutions available today for react to the DDoS attack. Those reactive mechanisms can be further divided into several classes:

4.2.1 Spoofing-based

For spoofing-based attacks, we need to identify the sources of attack traffic. This kind of approaches [4] [5] [6] try to figure out which machines attacks come from. Then appropriate measurement will be take on those machines (or near

them) and eliminate the attacks. In the case where attacker has a vast supply of machines, the trace approaches become not too helpful. A good example of the trace back technique is Traceback:

Traceback [4] is a technique for locating the agent machines making the DDoS attacks. It helps a victim to identify the network paths traversed by attack traffic without requiring interactive operational support from internet Service Providers. This approach is demonstrated in Figure 1. Each packet header may carry a mark, containing the EdgeID, represented by the IP address of the two routers forming an edge. This is used to specify an edge it has traversed. In addition, another field in the header is reserved to specify the distance from the edge to the victim.

Marking procedure at router R*:*
for each packet w
let x be a random number from [0..1)
if x < p then
write R into w.start and 0 into w.distance
else
if w.distance = 0 then
write R into w.end
increment w.distance
Path reconstruction procedure at victim v*:*
let G be a tree with root v
let edges in G be tuples (start,end,distance)
for each packet w from attacker
if w.distance = 0 then
insert edge (w.start,v,0) into G
else
insert edge (w.start,w.end,w.distance) into G
remove any edge (x,y,d) with d 6= distance from x to v in G
extract path (Ri..Rj) by enumerating acyclic paths in G
Figure 1: Traceback edge sampling algorithm

Routers mark the packets with some probability. And when a router decides to mark a packet, it writes its own address into the start field of the EdgeID and mark the distance field to zero. Otherwise, if the distance field is already zero this indicates that the packet was marked by the previous router. In this case, the router writes its own address into the end field of the EdgeID. Thus this represents the edge between itself and the previous router. In addition, if the router doesn't mark the packet then it always increments the distance field. This is important for assist in figure out the attacker spoofing those fields. The victim under attack reconstructs the path from the marked packets using the algorithm described in Figrue 1.

Strictly speaking, traceback does nothing to stop the DDoS attacks. Actually it only identifies attackers' true IP addresses within a subnet. If the IP spoofing are prohibited in the Internet, traceback would be of no use. The pro side of traceback is that it can be incrementally deployable, because edges are constructed only between participating routers. It is effective for non-distributed attacks and those highly overlapping attack paths. The information about the attack paths can help locating routers close to the source. Yet the con side of this approach is that packet marking incurs overhead at routers and reassembling the widely distributed attack paths is computational expensive. Furthermore, the path reassembly is quite complex and it is hard to make sure of its complete correctness. In addition, because the routers only mark the packet probabilistically, chances are that some of the packets are not marked at all. If those happen to be the spoofed packet from the attacker, they can produce false outcome.

4.2.2 Non-spoofing-based Filtering Based on Traffic Anomaly

Filtering and rate-limiting are the basis for most defensive approaches. This defense category addresses the core of the problem by limiting the amount of traffic presented to target. Filtering drops packets with particular characteristics. As long as the characteristics of the traffic are correctly identified, collateral damage can be low, but there is no guarantee that enough packets have been dropped. On the other hand, rate-limiting drops packets on basis of the amount of traffic. This technique does assure that target is not overwhelmed, but part of the legitimate traffic might also be dropped. Those filtering are done in the IP-layer.

4.2.2.1 Core-based Filtering

Pushback [7] [8] is a mechanism to preferentially drop attack traffic to relieve the congestion. Aggregate-based congestion control (ACC) that operates at the granularity of aggregates was proposed. An aggregate is a collection of packets from one or more flows that have some property in common. An example of aggregates are TCP SYN packets and ICMP ECHO packets. To reduce the impact of congestion caused by such aggregates, two related ACC mechanisms are used. The local aggregate-based congestion control (Local ACC), consists of an identification algorithm used to identify the aggregate(s) causing the congestion, and a control algorithm that reduces the throughput of this aggregate to a reasonable level. The second ACC mechanism, pushback, allows a router to request adjacent upstream routers to rate-limit the specified aggregates. Pushback prevents upstream bandwidth from being wasted on packets that are only going to be dropped downstream. In addition, for a DoS attack, if the attack traffic is concentrated at a few upstream links, pushback protects other traffic within the aggregate from the attack traffic. Yet on the other hand, Pushback only works in contiguous deployment and deployment requires modification of existing core routers and might need to purchase new hardware.

4.2.2.2 Edge-based Filtering

Egress filtering monitors and filters the packets that leave internal network to external network. Certain rules can be set up in the router to determine whether a packet should be filtered or not. If the packet pass all the rules, they are routed the sub-network. In DDoS attacks, the IP address of a packet are often be spoofed, thus there is a good probability that the spoofed source address of this packet is not a valid source address of that sub-network. When the firewall rule explicitly filters out all the traffic without an IP address originating from this subnet, those DDoS packets with spoofed IP source addresses will be discard.

In **ingress filtering**, packets coming into the network are filtered if the network sending it should not send packets from IP address of the originating computer. In order to do ingress filtering, the network needs to know which IP addresses each of the networks it is connected to may send. This is not always possible. For instance, a network that has a single connection to the Internet has no way to know if a packet coming from that connection is spoofed or not. Thus this requires that the ingress filtering deployed at the border of Internet Service Providers where address ownership is relatively unambiguous and traffic load is low. However, the success of ingress filtering requires widespread deployment. Yet up until now, the majority of ISPs are reluctant to implement this service because of the administrative complexity and potential overhead. In addition, even ingress and egress filtering are universally deployed, attackers can still forge addresses from the hundreds or thousands of hosts within a valid customer network [9].

4.3 DDoS Attack Solution Considerations

An ideal DDoS defense solution should have the following characteristics: effective, transparent to existing Internet infrastructure, low performance overhead, invulnerable to attacks aim at defense system, incremental deployable and no impact on the legitimate traffic. We will further discuss the solutions to DDoS attack based on those considerations.

4.3.1 Effectiveness

In the approaches for identify the source of attack traffic, *Traceback* facilitates locating routers close to the attack sources. Yet it does not work well for highly distributed attacks and its result is not 100% accuate. It is more effective for non-distributed attacks and for highly overlapping attack paths. Packet marks used in Traceback can be forged by the attackers. *PICA*, on the other hand, records paths of packet streams in path messages (sent as an ICMP message), thus eliminating the need of path reconstruction at the receiver end. This approach is more efficient in constructing the attacker map in DDoS.

4.3.2.Transparency to existing Internet infrastructure

Most of the approaches requires the changing of the Internet infrastructure, thus make the solution not so applicable. For example, the deployment of *pushback* requires modification of existing core routers and likely purchase of new hardware.

The use of overlay network provide an alternative approach. These approaches don't require to change the network protocol or routers. Such system uses Internet-wide network of nodes to act as a distributed firewall, and carry out authentication for the clients. The protected servers hide behind the overlay network, only authorized clients can access protected servers through the overlay network. Overlay network is nothing but a nontransparent way of packet interception. Once all incoming packets into a protected server can be intercepted, whether the server's identity is secret or not is immaterial.

4.3.3 Extent of modification to client-side software

Most of the solutions don't require the modification to client-side software, like Egress Filtering, Ingress Filtering NetBouncer etc. Yet the following solutions require the client-side change: In SOS, clients must be aware of overlay and use it to access the victim. When Client Puzzles are used, client modification is required to support receiving and solving the puzzles.

4.3.4 Performance overhead

Some of the approaches have little overhead, for example, in *Pushback*, the operation is simple and nearly no overhead for routers. In *traceback*, Packet marking incurs moderate overhead at routers. Yet Reassembly of distributed attack paths is prohibitively expensive, but this can be countered by doing the computation offline. When using the *Client Puzzles*, the puzzle verification consumes quite some of server resources.

4.3.5 Whether the defense systems themselves are vulnerable to attacks

Most of the approaches use the stateless way of operation. Thus attackers cannot launch state-consumption attack on these defense systems.

V. Conclusion

DDoS attacks are quite advanced and powerful methods to attack a network system to make it either unusable to the legitimate users or downgrade its performance. They are increasingly mounted by professional hacks in exchange for money and benefits. Botnets containing thousands of nodes impose a severe hazard to the Internet online business. Yet there seems to be no "silver bullet" to the problem. This survey examines the possible solutions to this problem, provides a taxonomies to classify those solutions and analyzes the feasibility of those approaches. Based on the analysis of existing

solutions, we proposed desirable solution to defend DDoS.

References

[1] N. Long S. Dietrich and D. Ddittrich, "Analyzing distributed denial of service tools: the shaft case," in *Proceedings of the LISA XIV*.

[2] Randal Vaughn and Gadi Evron, "Dns amplification attacks preliminary release," March 17 2006.

[3] Kevin J. Houle and George M. Weaver, "Trends in denial of service attack technology," http://www.cert.org/archive/pdf/DoS trends.pdf, October 2001.

[4] Stefan Savage, David Wetherall, Anna R. Karlin, and Tom Anderson, "Practical network support for IP traceback," in *SIGCOMM*, 2000, pp. 295–306.

[5] Alex C. Snoeren, Craig Partridge, Luis A. Sancheq, Christine E. Jones, Fabrice Tchakountio, Stephen T. Kent, and W. Timothy Strayer, "Hash-based ip traceback,"

[6] S. Bellovin, "Icmp traceback messages," http://www.research.att.com/ smb/papers/draft-bellovin-itrace-00.txt, 2000.

[7] John Ioannidis and Steven M. Bellovin, "Implementing pushback: Router-based defense against DDoS attacks," in *Proceedings of Network and Distributed System Security Symposium, Catamaran Resort Hotel San Diego, C alifornia 6-8 February 2002*, 1775Wiehle Ave., Suite 102, Reston, VA 20190, February 2002, The Internet Society.

[8] R. Mahajan, S. Bellovin, S. Floyd, J. Vern, and P. Scott, "Controlling high bandwidth aggregates in the network," 2001.

[9] Computer Emergency Response Team, "Cert advisory ca-2000-01 denial-of-servic developments," http://www.cert.org/advisories/CA-2000-01.html, January 2000.