DDOS ATTACKS AND DEFENSE MECHANISMS: A CLASSIFICATION

Christos Douligeris and Aikaterini Mitrokotsa

Department of Informatics
University of Piraeus, Piraeus, Greece
{cdoulig, mitrokat}@unipi.gr

ABSTRACT

Denial of Service (DoS) attacks are an immense threat to Internet sites and among the hardest security problems in today's Internet. Of particular concern - because of their potential impact - are the Distributed Denial of Service (DDoS) attacks. With little or no advance warning a DDoS attack can easily exhaust the computing and communication resources of its victim within a short period of time. This paper presents the problem of DDoS attacks and develops a classification of DDoS defense systems. Important features of each attack and defense system category are described and advantages and disadvantages of each proposed scheme are outlined. The goal of the paper is to place some order into the existing attack and defense mechanisms, so that a better understanding of DDoS attacks can be achieved and more efficient defense mechanisms and techniques can be devised.

1. INTRODUCTION

Denial of Service (DoS) attacks constitute a severe problem in the Internet. The impact of DoS attacks has been well demonstrated in the computer network literature. The main aim in the DoS is the disruption of services by attempting to limit access to a machine or service instead of subverting the service itself. This kind of attacks aims at rendering a network incapable of providing normal service by targeting either the network's bandwidth or its connectivity. These attacks achieve their goal by sending at a victim a stream of packets that swamps his network or his processing capabilities.

Distributed Denial of Service (DDoS) is a relatively simple, yet powerful, technique to attack Internet resources. DDoS attacks add the many-to-one dimension to the DoS problem making the prevention more difficult and the impact proportionally severe. There are no apparent characteristics of DDoS streams that could be directly and wholesomely used for their detection.

In this paper we try to introduce some structure to the DDoS field by presenting the problem of DDoS attacks and proposing a classification of the defense mechanisms that can be used to combat these attacks. In each defense mechanism we define special and important features and characteristics. Our purpose is to describe the existing problems so that a better understanding of DDoS attacks can be achieved and more efficient defense mechanisms and techniques can be devised.

This paper is organized as follows. Section 2 investigates the problem of DoS attacks and presents a classification of DoS attacks. Section 3 investigates the problem of DDoS attacks, presents a classification of DDoS attacks, section 4 proposes a classification of DDoS defense mechanisms, while section 5 concludes the paper.

2. DOS ATTACKS

A DoS attack can be described as an attack designed to render a computer or network incapable of providing normal services. A DoS attack is considered to take place only when access to a computer or network resource is intentionally blocked or degraded as a result of malicious action taken by another user. These attacks don't necessarily damage data directly, or permanently, but they compromise the availability of the resources.

DoS attacks can be classified as follows:

Network Device Level: DoS attacks in the Network Device Level include attacks that might be caused either by taking advantage of bugs in software or by trying to exhaust the hardware resources of network devices.

OS Level: In the OS Level DoS attacks take advantage of the ways operating systems implement protocols.

Application-based attacks: A great number of attacks try to settle a machine or a service out of order either by taking advantage of specific bugs in network applications that are running on the target host or by using such applications to drain the resources of their victim.

Data Flooding: An attacker may attempt to use the bandwidth available to a network, host or device at its greatest extent, by sending massive quantities of data and so causing it to process extremely large amounts of data.

Attacks based on protocol features: DoS may take advantage of certain standard protocol features, for

example several attacks exploit the fact that IP source addresses can be spoofed.

3. DDOS ATTACKS

3.1. Definition and strategy of DDoS attacks

A DDoS attack uses many computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the DoS significantly by harnessing the resources of multiple unwitting accomplice computers, which serve as attack platforms.

A DDoS attack is composed of four elements, as illustrated in Figure 1:

- The real attacker.
- The handlers or master compromised hosts, who are capable of controlling multiple agents.
- The attack daemon agents or zombie hosts, who are responsible for generating a stream of packets toward the intended victim.
- A victim or target host.

A DDoS attack can be described as follows:

Recruitment: The attacker chooses the vulnerable agents, which will be used to perform the attack.

Compromise: The attacker exploits the vulnerabilities of the agents and plants the attack code, protecting it simultaneously from discovery and deactivation.

Communication: The agents inform the attacker via handlers that they are ready.

Attack: The attacker commands the onset of the attack.

Sophisticated and powerful DDoS toolkits are available to potential attackers increasing the danger of becoming a victim in DoS or DDoS attack. Some of the most known DDoS tools are Trinoo, TFN, Stacheldraht, TFN2K, mstream and Shaft.

3.2. DDoS attack classification

There are two main classes of DDoS attacks (Figure 2): 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 victim system. Bandwidth attacks can be divided to flood attacks and amplification attacks. A resource depletion attack is an attack that is designed to tie up the resources of a victim system. This type of attack can be divided to protocol exploit attacks and malformed packet attacks.

DDoS attacks can also be classified in two general categories: direct attacks and reflector attacks. Direct attacks have already been described in the previous section. A reflector is an indirect in which intermediary nodes, are used as attack launchers. A reflector is any IP host that will return a packet if sent a packet.

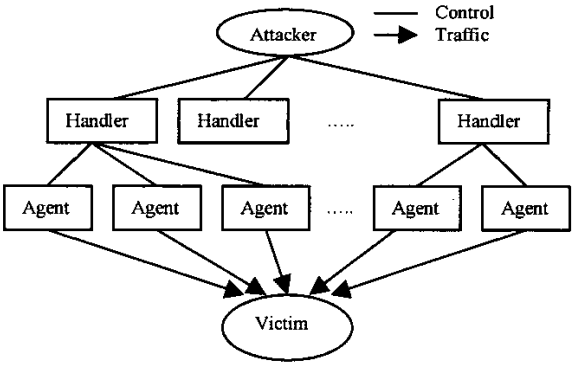

Figure 1- Architecture of DDoS attacks

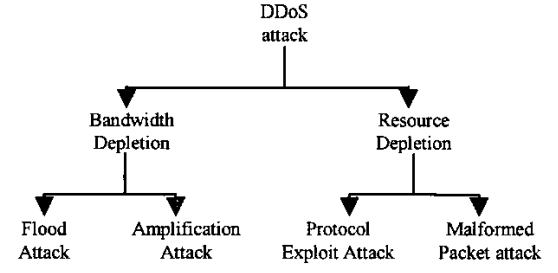

Figure 2 - DDoS attack classification

4. CLASSIFICATION OF DDOS DEFENSE MECHANISMS

We present two classifications of DDoS defense mechanisms according to different criteria. The first classification categorizes the DDoS defense mechanisms depending on the activity deployed and the second classification divides the DDoS defenses according to the location deployment. We describe in detail the DDoS defenses in the first classification and just refer to the DDoS defenses and the way they are categorized in the second classification.

4.1. Classification by activity

4.1.1. Intrusion Prevention

The best mitigation strategy against any attack is if the attack never occurs. There are many DDoS defense mechanisms that try to prevent systems from attackers:

Using globally coordinated filters. Ingress Filtering, proposed by Ferguson and Senie [1], is a restrictive mechanism to drop traffic with IP addresses that do not match a domain prefix connected to the ingress router. Egress filtering is an outbound filter, which ensures that only assigned or allocated IP address space leaves the network. Egress filters do not help to save resource wastage of the domain where the packet is originated but

they protect other domains from possible attacks. Route-based filtering, proposed by Park and Lee [2], uses the route information to filter out spoofed IP packets.

Disabling Unused Services. If network services are unused, the services should be disabled to prevent attacks.

Applying Security Patches. The host computers should update themselves with the latest security patches for the bugs present and use the latest techniques available to minimize the effect of DDoS attack.

Changing IP address. A solution, practical only for local DDoS attacks, is called "moving target defense", in which we invalidate the victim computer's IP address by changing it with a new one. Once the IP address is changed, edge routers drop the attacking packets.

Disabling IP Broadcasts. By disabling IP broadcasts host computers can no longer be used as amplifiers in ICMP Flood and Smurf attacks.

Creating client bottlenecks. These remedies try to create bottleneck process on Zombie computers and limit their attacking capability. RSA's Client Puzzles algorithm and Turing test need the client to do some extra computation before setting up a connection.

4.1.2. Intrusion Detection

Intrusion detection systems detect DDoS attacks by using the database of known signatures or by recognizing anomalies in system behaviors.

- **Anomaly detection**

Anomaly detection relies on detecting behaviors that are abnormal with respect to some normal standard. Many anomaly detection systems and approaches have been developed to detect the faint signs of DDoS attacks.

A scalable network monitoring system called NOMAD [3] is able to detect network anomalies by making statistical analysis of IP packet header information. Lee and Stolfo [4] use data mining techniques to discover patterns of systems features that describe program and user behavior and compute a classifier that can recognize anomalies and intrusions.

Cabrera et al. [5] propose a Network Management System for the detection of DDoS attacks in which key variables are chosen with a statistical analysis, to achieve the early detection of the attack.

A mechanism called congestion triggered packet sampling and filtering is proposed by Huang et al. [6]. According to this approach, a subset of dropped packets due to congestion for statistical analysis is selected. If anomaly is indicated by the statistical results, a signal is sent to the router to filter the malicious packets.

Gil et al. [7] propose a heuristic data-structure, which postulates if the detection of IP addresses that participate in a DDoS attack is possible, and then measures could be taken to block only these particular addresses. This approach cannot prevent proportional attacks nor can it detect DDoS attacks that use many zombies.

- **Misuse detection**

Misuse detection identifies well-defined patterns of known exploits and then looks out for occurrences of such patterns. Several popular network monitors perform signature-based detection, such as CISCO's NetRanger, NID, RealSecure, Snort.

4.1.3. Intrusion Response

Once an attack is identified, the immediate response is to identify the attack source and block its traffic accordingly. There are many approaches that target in tracing and identifying the real attack source.

IP traceback traces the attacks back towards their origin, so one can find out the true identity of the attacker and, achieve path characterization. Some factors that render IP traceback difficult is the stateless nature of Internet routing and the lack of source accountability in TCP/IP protocol.

ICMP traceback has been proposed by Bellovin [8]. According to this mechanism every router samples the forwarding packets with a low probability and sends an ICMP traceback message to the destination. If enough traceback messages are gathered at the victim, the source of traffic can be found by constructing a chain of traceback messages. In order to face DDoS attacks by reflectors, Barros [9] proposes a modification of ICMP traceback messages. In this approach, routers send ICMP messages to the source of the currently being processed packet rather than its destination.

A **link-testing traceback** technique is proposed by Burch and Cheswick [10]. It infers the attack path by flooding the links with large burst of traffic and examines whether this induces any perturbation on that network. If so, this link is probably a part of attack path.

CenterTrack [11] is an architecture proposed by Stone, which creates an overlay network of IP tunnels by linking all edge routers to central tracking routers, and all suspicious traffic is rerouted from edge routers to the tracking routers.

Probabilistic Packet Marking was originally introduced by Savage et al [12] who described efficient ways to encode partial route path information and include the traceback data in IP packets. Song and Perrig [13] improved the performance of PPM and suggested the use of hash chains for authenticating routers. This marking scheme is efficient and accurate in the presence of a large numbers of DDoS attacks.

Hash-based IP traceback has been proposed by Snoeren, et al. [14]. This technique uses a Source Path Isolation Engine (SPIE) which generates audit trails of traffic and can trace origin of single IP packet delivered by a network in recent past.

4.1.4 Intrusion Tolerance

Intrusion tolerant research accepts that it is impossible to

prevent or stop DoS completely and focuses on minimizing the attack impact and on maximizing the quality of its services. Intrusion tolerance can be divided in two categories: fault tolerance and quality of service.

The idea of fault tolerance is that by duplicating the network's services and diversifying its access points, the network can continue offering its services when one network link is congested by flooding traffic.

Quality of Service (QoS) describes the assurance of the ability of a network to deliver predictable results for certain types of applications or traffic. Among frameworks to provide Internet QoS, Integrated and Differentiated Services have emerged as the principal architectures.

Various autonomous architectures have been proposed that demonstrate intrusion tolerance during DDoS bandwidth consumption attacks. Characteristic examples of Intrusion Tolerant QoS systems are the XenoService [15] and the pushback architecture [16].

4.2. Classification by Deployment Location

Based on the deployment location, we divide DDoS defense mechanisms to the following categories:

Victim-Network Mechanisms: Most of the systems for combating DDoS attacks have been designed to work on the victim side, since it suffered the greatest impact of the attack. Examples of these systems are resource accounting, and protocol security mechanisms.

Intermediate-Network Mechanisms: DDoS defense mechanisms deployed at the intermediate network are very effective since the attack can be handled easily and traced back to the attackers. Examples of these mechanisms are traceback [8] and pushback [16].

Source Network Mechanisms: DDoS defense mechanisms at the source network can stop attack flows before they enter the Internet core and before they aggregate with other attack flows. An example of these mechanisms is proposed in [7].

5. CONCLUSION

Undoubtedly, DDoS attacks are a serious problem for which numerous defense mechanisms have been proposed. In this paper, we tried to present a methodology that would allow a classification of the DDoS attack problem in order to be able to find more effective solutions.

One great advantage of the development of DDoS attack and defense classifications is that effective communication and cooperation between researchers can be achieved so that additional weaknesses of the DDoS field can be identified. Their value in achieving further research and discussion is undoubtedly large. A next step in this path would be to create sets of data and an experimental testbed so that all these various mechanisms can be compared and evaluated.

6. ACKNOWLEDGEMENTS

This work has been partially supported by the University of Piraeus Research Center.

Due to the short nature of the paper the full list of references can be found at:
http://rainbow.cs.unipi.gr/~p97032/DDoSattacks.pdf.

7. REFERENCES

[1] P. Ferguson and D. Senie, "RFC 2827: Network Ingress Filtering: Defeating Denial of Service attacks which employ IP source Address Spoofing", May 2000.

[2] K. Park and H. Lee, "On the effectiveness of probabilistic packet marking for IP traceback under Denial of Service attack", Proc. IEEE INFOCOMM, Anchorage, AK, USA, pp. 338-347, Apr. 2001.

[3] R. R. Talpade, G. Kim and S. Khurana, "NOMAD: Traffic-based Network Monitoring Framework for Anomaly Detection", Proc. 4th IEEE Symposium on Computers and Communications, Ted Sea, Egypt, pp. 442-451, June 1999.

[4] W. Lee and S. J. Stolfo, "Data mining approaches for intrusion detection", 7th USENIX Security Symposium, San Antonio, TX, pp. 79-93, January 1998.

[5] J. B. D. Cabrera et al., "Proactive Detection of Distributed Denial of Service Attacks using MIB Traffic Variables – A Feasibility Study", Proc. 7th IFIP/ IEEE Int. Symp. On Integrated Network Management, Seattle, WA, May 2001.

[6] Y. Huang, J. M. Pullen, "Countering Denial-of-Service attacks Using Congestion Triggered Packet Sampling and Filtering", Proc. 10th ICCCN, Arizona, USA, Oct. 2001.

[7] T.M. Gil and M. Poleto, "MULTOPS: a data-structure for bandwidth attack detection", Proc. 10th USENIX Security Symposium, Washington, DC, pp.23-38, Aug. 2001.

[8] S. M. Bellovin, "ICMP traceback messages", Internet Draft, 2001.

[9] C. Barros, "A proposal for ICMP traceback messages", Internet Draft, Sept. 2000.

[10] H. Burch and H. Cheswick, "Tracing anonymous packets to their approximate source", Proc. USENIX LISA, New Orleans, pp.319-327, Dec. 2000.

[11] R. Stone, "CenterTrack: An IP OverlayNetwork for Tracking DoS Floods", Proc. 9th USENIX Security Symposium, Denver, Colorado, pp.199-212, Aug. 2000.

[12] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Network support for IP traceback", Proc. IEEE/ACM Transaction on Networking, vol. 9: (3), pp. 226-237, June 2001.

[13] D. X. Song and A. Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback", Proc. IEEE INFOCOMM, Anchorage, AK, USA, pp. 878-886, Apr. 2001.

[14] A. C, Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, and T. Strayer, "Single-Packet IP Traceback", IEEE/ACM Transactions on Networking (ToN), vol. 10: (6), pp. 721-734, Dec. 2002.

[15] J. Yan, S. Early, R. Anderson, "The XenoService – A Distributed Defeat for Distributed Denial of Service", Proc. Info. Survivability Workshop, Boston, USA, Oct. 2000.

[16] J. Ioannidis, S. M. Bellovin, "Implementing Pushback: Router-Based Defense Against DDoS Attacks", Proc. IEEE INFOCOMM, Anchorage, AK, USA, pp. 878-886, Apr. 2001.