AN INTROSPECTIVE VIEW OF DENIAL OF SERVICE (DOS): DETECTION, PREVENTION, AND MITIGATION

Hak J. Kim
Hofstra University, Department of IT/QM, 134 Hofstra University, Hempstead, USA
Hak.J.Kim@hofstra.edu

ABSTRACT

Growth and advancements in technology have paved the way for people to have unlimited connectivity, but with this limitless connection to the Internet and extensive use of online resources there are many chances for malicious activities including hacking attacks. One of the most popular types of attacks in the Internet is Denial of Service (DoS). The DoS attack is an attack to make the company’s resources unavailable to the user with ease and little or no cost to the attacker. This attack is very real and is becoming popular. This paper discusses the DoS attacks and then investigates methods and techniques to detect, prevent, and mitigate malicious DoS attacks.

Keywords: Denial of Service (DoS), Detection, Prevention, Mitigation

1. INTRODUCTION

In today’s Internet-connected world, many firms depend on electronic connectivity to facilitate operation, management, and services in a timely manner. However, this connectivity is either degraded or prevented because of vulnerable characteristics of the Internet including scalable and flexible architecture. The Denial of Service (DOS) attacks are one of the most widely spread problems faced by most of the Internet Service Providers (ISP’s) today. In this regard, protecting networks against DoS attacks is a must for all organizations in order to secure their IT assets. Implementing such protection mechanisms involve certain steps such as DoS detection and the application of appropriate prevention and mitigation techniques.

The studies show Denial of Service (DoS) attacks ranking as high as Internet outages and hacker attacks as the greatest online vulnerability. The DoS attack is an attack to make the company’s resources unavailable to the user with ease and little or no cost to the attacker. This attack is very real and is becoming popular. Since these attacks will result in reduction in profit, loss of customers, and communicate with customers. In the summer of 2008, the DoS attacks on Georgian government websites were used to paralyze their decision making process while Russian troops invaded part of the country (Korns and Kastenberg, 2009). Additionally, in the 2011, there have been several DoS attacks, called Operation Ababil, on US financial institutions originating from hackers based in Iran.

Internet Service Providers (ISPs) are challenged with the task of preventing the DoS attacks toward their customers. The DoS disruption comes in many forms, such as overwhelming available connections, exploiting application vulnerabilities, and attempting to bring down the physical IT environment (AL-Musawi, 2012).

This paper is to present about the DoS attacks and explore several methods of combating DoS, describe and analyze the techniques used to detect, prevent, and mitigate.

2. DENIAL OF SERVICE: A BRIEF OVERVIEW

The DoS attack can hamper Internet operations by blocking connections with an inundation of messages that overwhelm the system or create a bottleneck that prevents legitimate traffic from getting through. It does not put your information at risk of exposure, but rather brings down a website or servers that would prevent the system from operating and being accessible to its users. There are a number of DoS attacks that exist and can carry out its agenda by brute-
force floods of messages that affect the network in certain ways. The ping command is one that is used to try to link two computers. However, during a ping flood attack, the amount of messages overwhelms the receiving computer with the amount of messages request that it gets. The following is a simple example command:

C:\Users\X> ping 192.168.00 -n 5 -l 65500

The initiating computer can send an enormous amount of request to the receiving computer that would make that system freeze because it cannot handle the amount of data being received. In this example of a ping flood, the –n instructs the prompt to launch a message a certain amount of times. The capacity for the receiving computer was, in this case, was four packets and five were sent. The -l instructs the prompt to dispatch the amount of data that each packet will contain.

The example above is a small description of how the DoS attack can be carried out with one computer affecting another. For networks and websites the capacity to handle data is more robust and as such, it would require a larger effort in order to crash the server or router. A Distributed Denial of Service (DDoS) is more commonly used for larger networks. The concept is the same as a ping flood, only that for the DDoS, numerous computers are used at a given time often without their respective owners knowing that this is happening. The most common way that this can be accomplished is to introduce a Virus or Trojan that would allow an attack to be orchestrated without the knowledge of the computer owners. This would render the computer systems as zombies and allow a hacker to flood a server with numerous request sent at one time from different machines.

The DoS attacks aim at exhausting computer networks and systems resources or reducing their performances in order to prevent them from delivering the applications and services that they are designed for. Those attacks are possible for the attackers to perform because of possible vulnerabilities that can be found in computer and network systems. Typically, in the case of the DDoS attack, the attacker would install malware on some hosts on the Internet to have them under control; those hosts can be classified into two categories: the handlers that will be directly controlled by the attacker and acting as a relay to control the attack agents that will be performing synchronized attacks to the targeted network or system (see illustration below).

Among those DoS attacks, several categories exist such as those which cause flooding to the targeted systems using common layers 3 or 4 network protocols (e.g. TCP, UDP or ICMP). In a non-exhaustive manner, flooding attacks can for instance be direct when the attacker sends IP packets to the target system directly or indirect when he or she hijacks the IP address of that target to send request to other several systems; those systems will therefore respond to the victimized machine with a large range of responses at the same time; which will flood it. Another possibility is to hijack the TCP three-way handshake initialization process causing a TCP SYN attack with the consequence that the victimized machine will be overloaded and not able to handle new TCP session requests. Last category of DoS attack one would talk about, is fragmentation attacks that are not only often used by attackers to bypass IDSs that will not detect them, but will cause the targeted systems to put too much resources in the reassembly of the fragmented packets (Glenn, 2003).

3. DETECTION, PREVENTION, AND MITIGATION

There are various methods and techniques for detecting, preventing, and mitigating the DoS attacks. We investigate and discuss these methods and techniques to gain an appreciation of the processes needed to form an adequate defence for the network systems.

3.1 Detection

The DoS attacks can be performed through low rate methods, where the attacker sends packets periodically to the victimized system; the period of sending such packets can be calculated based on the concerned system’s Retransmission TimeOut, so that when the system is ready to retransmit packets after the timer expiry, it is flooded again by new request packets to process; as those low rate attacks are not full time attacks, they are hardly detectable by IPS/IDS (Mathew & Katkar, 2011).

The preconized detection technique for that low rate DoS can be the dynamic detection that consists of several steps, among which one can quote sampling and normalizing...
incoming traffic in order to differentiate low rate attack traffic from normal traffic; the next step will be to filter noise for instance by comparing traffic destined to the victimized network to other destination traffic. This will serve for the two steps that deal with traffic feature and signature determination to characterize the kind of traffic that is carried on the network. Those two elements will then be compared to low rate DoS attack and make a decision (Sun, Lui & Yau, 2004).

An additional detection technique applicable to DDoS attacks that is named FireCol is made of the implementation of IPS virtual rings surrounding the systems to protect. In such a configuration, the system to protect sends protection request to the nearest IPS that do the same with next hop IPSs in a vertical way; on the other side, IPSs on the same virtual ring exchange information on potential attacks based on attacks detection probability or scores; that attack probability itself being determined taking into consideration the total traffic bandwidth directed to a particular client (in this case, a potential victimized system) compared to the normal bandwidth it can support. The detection system protects its clients based on parameters such as IP traffic pattern, ports or protocols in use (François et al., 2012).

A method preconized for early DoS detection is the k-NN (k-nearest neighbor) one. In this method, the system to protect is classified into three possible states regarding potential DoS attacks (normal, pre-attack, attack); each state is characterized by a set of parameters, including among others source and destination IP addresses, used port numbers, protocol types (e.g. TCP, UDP, ICMP), that are computed during a time period. The K-NN algorithm will therefore determine the probable next stages of the concerned parameters using its k-nearest neighbor logic; this will lead to the determination of the probable next state of the system to protect; which helps in early the detection of DoS attacks (Nguyen & Choi, 2010). More papers for detecting the DoS attacks are summarized in Table 1.

### Table 1. Summary of Detection Papers

<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sun, Lui &amp; Yau (2004)</td>
<td>Defending Against Low-rate TCP Attacks: Dynamic Detection and Protection</td>
<td>Proposing a distributed detection mechanism which uses the dynamic time warping method to robustly and accurately identify the existence of high-rate attack sources.</td>
</tr>
<tr>
<td>Akella, Bharambe, Reste, &amp; Seshan (1999)</td>
<td>Detecting DDoS Attacks on ISP Networks</td>
<td>Reporting the detection of DDoS flooding attacks from an Internet Service Provider (ISP) perspective the effects and how to detect such malicious attacks on individual ISP networks.</td>
</tr>
<tr>
<td>Wang, Wang, &amp; Su (2011)</td>
<td>A New Multistage Approach to detect subtle DDoS Attacks</td>
<td>Applying statistical analysis of traffic using a local DDoS sensor, then create a DDoS algorithm to detect attacks.</td>
</tr>
<tr>
<td>Lee, Kim, Lee, &amp; Park (2012)</td>
<td>Detection of DDoS attacks using optimized traffic matrix</td>
<td>Proposing an enhanced DDoS attack detection approach by optimizing the parameters of the traffic matrix using a Genetic Algorithm (GA) to maximize the detection rates.</td>
</tr>
<tr>
<td>Blauel, Hongyong, Boris, &amp; Alexandre (2001)</td>
<td>A Novel Approach to Detection of “Denial-of-Service” Attacks via Adaptive Sequential and Batch-Sequential Change-Point Detection Methods</td>
<td>Presenting the idea of anomaly based Intrusion Detection, which employs adaptive and batch-sequential algorithms as a method of detecting DoS attacks because they are self-learning, meaning that they have the autonomy to adjust themselves based upon variation in network traffic and usage patterns.</td>
</tr>
<tr>
<td>Dong, Yeong, Sun, &amp; Fangchun (2012)</td>
<td>A Precise and Practical IP Traceback Technique Based on Packet Marking and Logging</td>
<td>Proposing a precise IP traceback approach with low storage overhead, which improves accuracy and practicality greatly.</td>
</tr>
</tbody>
</table>

### 3.2 Mitigation

The proper DoS resolution cannot rely solely on improved processors in order to be able to handle higher volumes of server requests. They also state, hiding DNS and web services servers from external sources often involve increased hardware costs, increased implementation costs, increased public Internet traffic and delay in user requests are they never go directly to the intended server. A proper resolution also cannot require significant amount of processing power or it will become a bottleneck for normal network traffic, not to mention a target of an unintentional DDoS flood attack (Wade et al, 2010).

Another mitigation mechanism consists of blocking IP sources for those of the addresses that are involved in potential attacks; this can be detected by identifying IP addresses that are originating higher traffic directed to the potential victim system in combination with some heuristic assumptions based on criteria such as the differential between incoming and outgoing traffic to the target, the signature of recorded and known attacks and unknown IP addresses (François, Aib, & Boutaba, 2012).
The third mitigation technique suggested for that method, still based on packets marking, deals with the use of IP datagrams TTL (Time To Live) to mark them when crossing routers. Likewise, that technique helps detect DDoS traffic signature and therefore appropriate filtering methods can be applied to drop DDoS traffic packets to control the situation and improve the concerned network’s bandwidth and systems responsiveness (Nguyen & Choi, 2010).

In the fourth paper, Al-Musawi (2012) begins by explaining what DoS attacks are and how they affect the host and internet. He believes there are a couple main reasons why individuals are attracted to DoS attacks. First, there are tools out on the open market that can be used for attacking purposes; another reason is that it usually is untraceable so the individual can be anonymous. Regardless of the purposes, DoS attacks will be around because there are always going to be vulnerable targets. The author goes into great detail about using IP tables as a solution for mitigating and defending against DoS attacks. IP tables are part of the Linux Kernel that contains rules that control the packet filtering.

Administrators have rights and the ability to change the rules for the filtering, so the rules can start out simple but then change to complex by adding more of them. Al-Musawi believes that if you add too many rules it will be bad for the network and end users. Using Wireshark and a victim host, Al-Musawi was able to perform and complete some testing of his own. He concluded that using IP tables to set rules will be beneficial in helping to mitigate against DDoS/DoS attacks. Using route sets will allow it to determine whether traffic is authorized or unauthorized for the network.

In the last paper, Yu, Fang, Lu, & Li (2010) suggest trust management helmet (TMH) as a partial answer to this problem, which is a lightweight mitigation mechanism that uses trust to distinguish genuine users from assailants. The authors developed a strategy to defend against DDoS attacks based on the trust level developed by users. This trust level is based on previous activity of users that’s tracked in the following ways: short-term trust (recent user behavior), long-term trust (based on historical data collected on specific users), negative trust (calculated distrust of users), and Misusing Trust (calculation based on attempts of users to circumvent or develop false levels of trust.) These trust factors are combined for a trust value that is used to determine what priority to service requests. Additionally, if a user’s trust is found to be below a set threshold, that user is blacklisted, to prevent additional load and overhead needed to track potentially malicious requests. TMH is deployed at the server. Before a request is processed by the server it passes through the TMH. TMH checks the users trust level and determines if the request should be processed and at what priority. TMH finally updates the trust level of the requestor to be taken into account with future requests. Data on trust for each user is stored encrypted in a cookie on the user’s client. This serves as both an identification of the user as well as providing trust management data.

More DoS mitigation methods are summarized in Table 2.

### Table 2. Summary of Mitigation Papers

<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wade, Fujimori, Coffman, Feener, &amp; Haack (2010)</td>
<td>A Cross-Layer Approach for Mitigating Denial of Service Attacks: Device-Driven Filter and Remote Firewall</td>
<td>Presenting two methods to mitigate distributed denial of service attacks and flash crowds driver level packet filtering and remote firewall. Device driver level packet filtering is designed to eliminate harmful network traffic before it consumes the processing resource for higher network protocol layers at a production server.</td>
</tr>
<tr>
<td>Fransoni, Ailtb, &amp; Bousaba (2012)</td>
<td>Forcel – a collaborative protection network for the detection of flooding DDoS attacks</td>
<td>Presenting the evaluation of FireCol using extensive simulations and a real dataset. FireCol is an intrusion prevention systems (IPSs) located at the Internet service providers (ISPs) level.</td>
</tr>
<tr>
<td>Rivera (2005)</td>
<td>A stochastic estimator/detector for mitigating denial of service attacks</td>
<td>Defining an efficient formulation of a bad packet detector. This formulation specifies automated software which can update the firewall filter in real time to mitigate a distributed denial of service attack.</td>
</tr>
<tr>
<td>Garg &amp; Reddy (2004)</td>
<td>Mitigation of DoS attacks through QoS regulation</td>
<td>Presenting the resources to be protected and by controlling the depletion of resources for each class of traffic, then a certain amount of resources can be allocated to other areas that bypass depletion and allow other classes to continue receiving service.</td>
</tr>
<tr>
<td>Li &amp; Li (2010)</td>
<td>An adaptive approach for defending against DDoS attacks</td>
<td>Introducing an adaptive approach, which is used for defending against DDoS attacks, based on normal traffic analysis. The approach can check DDoS attacks and adaptively adjust its configurations according to the network condition and attack severity.</td>
</tr>
<tr>
<td>Goldstein, Reit, Stahl, &amp; Brenel (2008)</td>
<td>High Performance Traffic Shaping for DDoS mitigation</td>
<td>Presenting a Distributed Denial of Service (DDoS) attack mitigation system using traffic shaping where the bandwidth limit is defined by the probability of a source to be a legal user.</td>
</tr>
<tr>
<td>Garg (2011)</td>
<td>DDoS mitigation techniques-a survey</td>
<td>Discussing on Distributed Denial of Service attack, surveys, classifies and also systematically analyzes the various proposed mitigation techniques during the last decades by the researchers.</td>
</tr>
<tr>
<td>Yu, Fang, Lu, &amp; Li (2010)</td>
<td>Mitigating application layer distributed denial of service attacks via effective trust management</td>
<td>Proposing trust management helmet (TMH) as a partial solution to this problem, which is a lightweight mitigation mechanism that uses trust to differentiate legitimate users from attackers.</td>
</tr>
</tbody>
</table>

### 3.3 Prevention Methods

The first type of prevention mechanism for low rate DoS attacks can be to randomize the value of the network systems RTO values in order to hinder any possibility for the attacker to synchronize low rate DoS attacks periods on RTO values; in that case, the attack will be performed as a normal DoS attack detectable by an IPS/IDS system (Mathew & Katkar, 2011).

Second, a solution proposed by Kline, Afanasyev & Reicher (2011) to prevent DoS and DDoS attacks is the creation of a third-party network that will act as a shield node to protect the desired network against DoS or DDoS attacks. Typically, that third-party network will offer on-demand DoS shield services to client networks and systems to protect in such a way that when a client network detects a pre-attack sign, it can reroute its incoming traffic to that shield node that will filter it before resending it back to the destination network. That proposed solution has the advantage of easy deployment, since no major investment is required; however, diverting traffic to a third-party network may in the medium and long run pose certain problems such as bandwidth.
congestion and latency if that third-party infrastructure is not correctly designed to handle multiple clients’ traffic; another issue with it can be linked to security if that network is not trusted enough to filter traffic for other parties.

Third, Anderson et al. (2012) propose an end to end solution to allow traffic to be validated for legitimacy. Despite the advance of detection and filter to battle DDoS attack, it still does not give a reliable way to differentiate attack traffic from legitimate traffic. The authors of the paper propose all traffic to be tagged by a singles use token issued by the source and destination. The token will come in the form of a certificate that request by the source host. The final destination host will grant the certificate back to the host who request it. One of the great advantages of this is to use existing Internet infrastructure by deploying Request-To-Send (RTS) servers at each organization boundaries. The servers, in conjunction with verification points (VPs) alone the internet infrastructure, provide an infrastructure to allow identification of legitimate traffic. The VPs provide access control by examine traffic that tagged with the certificate. The RTS servers grant the token to the source host. The RTS server can be integrate with the existing BGP infrastructure. The RTS servers can propagate its information with the BGP advertisement. The use of RTS servers local configuration or BGP advertisement assure that the RTS servers only communicate to a legitimate RTS server. The RTS server and APs at the ingress / egress point of a network allow company control the level of participation by allowing the RTS server advertise via the BGP protocol. This method does not require any ISP interference or router configuration change.

to achieve success, specific detection, prevention or mitigation technique are required. However, while those methods are specific to that particular attack type, many share the same fundamental concepts which can be applied generically to different situations. In general, one technique is not sufficient to protect against multiple attack vectors, therefore, a broad range of techniques are required to offer a full range of protection. Unfortunately, as more techniques are added the chances for latency delays or introducing new attack vectors also increases.

4.2 Difficulty of Detecting Malicious Traffics

Many approaches to dealing with the DoS attack involve throttling down traffic, dropping packets and the like. These approaches do not seek to determine what traffic is legitimate what is malicious, thus legitimate traffic is impacted even as the attack is addressed. Detecting and mitigating DoS attacks can be difficult because determining which traffic is malicious and which is legitimate is not a straightforward problem. The articles above each contribute to the problem with solutions involving historic user behavior and other available data in IP headers (TTL). Using these tools each has developed reasonable contributions to the overall problem of detecting and mitigating these types of attacks.

5. CONCLUSIONS

Cybersecurity is a must for a safer cyberspace; as shown all along this paper, cyber threats like the DoS attacks can seriously endanger IT assets of any organization if not adequately controlled. In this regard, the investigated detection, prevention and mitigation techniques can perform if adequately implemented. However, we recognize that a single technique can hardly overcome the DoS attacks. It is therefore recommended to implement a combination several techniques in the philosophy of a defense in-depth system aiming at hindering any kind of cyber-attacks (Chen & Walsh, 2009). Moreover, working in collaboration among ISPs to counter the DoS attacks is a necessity since most techniques presented in this paper appeal to a collaborative framework for their efficient implementation.

In this paper, we have looked at several techniques for detection, prevention and mitigation of the DoS attacks. Each method is designed to protect against a specific occurrence in a specific network setup. However, there are commonalities between them. All defensive mechanisms essentially do the same thing; detect the attack and then do something to stop it. Detection is not always easy because one must differentiate legitimate from malicious traffic. Then once detected, the issue becomes how to stop the attack without impacting legitimate users. The catch-22 is that if technique impacts legitimate users, it has effectively helped the attacker achieve their goal. This is why there is much knowledge on these DoS attacks and research continues to look for new methods of protection.

<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mathew &amp; Katkar</td>
<td>Survey of low rate DoS attack detection mechanisms</td>
<td>Presenting the survey of techniques available for detecting low rate DoS attacks and compares them using various parameters.</td>
</tr>
<tr>
<td>Kline, Afanasyev &amp; Reiner</td>
<td>Shield: DoS filtering using traffic deflecting</td>
<td>Introducing a novel method that overcomes these issues, allowing a small number of deployed DoS defenses to act as secure on-demand shields for any node on the Internet.</td>
</tr>
<tr>
<td>Anderson, Roscoe, &amp; Wetherall</td>
<td>Preventing Internet denial-of-service with capabilities</td>
<td>Proposing a new approach to prevent and constrain denial-of-service (DoS) attacks. This method must first obtain permission to send from the destination; a receiver provides tokens, or capabilities, to those senders whose traffic it agrees to accept.</td>
</tr>
</tbody>
</table>

Table 3. Summary of Prevention Papers

4. ISSUES AND CHALLENGES

4.1 Variety of the DOS Attacks

The DoS attack is very difficult to defend because it can occur at any layer of the OSI model and can utilize varying methods
REFERENCES


