Crossroads
The ACM Student Magazine

Tracing the Development of Denial of Service Attacks: A Corporate Analogy

by ***Yanet Manzano***

Introduction

Over the last ten years, the number of Internet hosts has grown at an accelerated rate; slowdowns and traffic jams are plaguing the information superhighway. Consequently, companies struggle to meet the rising demand for speedy quality service. Unfortunately, the control mechanisms available today are not enough to handle the congestion problem we currently face. When we talk about the causes of congestion today, we have to decompose them into two major categories: one is congestion caused by legitimate traffic, and the other is congestion caused by malicious activities. In this article, we are going to focus on congestion created by malicious activities, specifically Denial of Service (DOS) Attacks.

DOS attacks are much like any other hacking attack, except that the penetration step does not exist. Because of this, most people consider DOS attacks as less of a threat, and therefore do not take enough preventive measures, until they find themselves facing a system shutdown and losses of millions of dollars. According to a CBI/FBI 2002 survey, the highest reported financial losses due to a single DOS attack increased from $1 million in 1998 to $50 million in 2002 [**8**]. In spite of such evidence, most companies still overlook the relevance of using preventive mechanisms to deal with DOS attacks. We have decided to place the situation in a different light, with the objective to provide a better understanding of the growing damage potential of this type of attack.

We are going to focus on a scenario in which an attacker individually launches his own company. The business would consist of launching DOS attacks against other companies, with profits being equivalent to the financial damages created by the DOS attacks launched. Our attacker starts with the traditional DOS model of one-attacker/one-victim, and then works to develop more sophisticated models that result in more damaging, and therefore more profitable attacks. Through this scenario, we will explore the three largest transformations of a DOS attack, from the traditional model to distributed DOS (DDOS), and to distributed DOS with reflectors (DRDOS). Before we move to trace the development of our attacker, we will explore some of the most famous DOS attacks that served him as inspiration to create his DOS Attack company.

DOS Hall of Fame: A Walk Through the Past

Before we move on, we will take a brief walk into the DOS Attack Hall of Fame to explore some of the most well-known DOS attacks documented in literature. These attacks, although not as powerful as they once were, still serve as inspiration for the new techniques behind the DOS attacks we face today.

1. **Ping of Death**:
   Creates a packet that exceeds the maximum 65,536 bytes of data allowed by the IP (Internet Protocol) specification, causing the computer that receives the packet to crash, hang, or reboot. Today, most operating systems have fixed the problem of dealing with oversized packets [**3**].
2. **Teardrop**:
   During its journey through the Internet, a packet may be broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that states, for instance, "This fragment is carrying bytes 600 through 800 of the original (non-fragmented) IP packet." The Teardrop attack creates a series of IP fragments with overloading offset fields, causing some systems to crash, hang, or reboot when the fragments are reassembled at the destination host [**5**].
3. **Smurf Attack**:
   This particular attack is what we call a brute force attack, targeted at the feature in the IP specification known as direct broadcast addressing. It floods the router with Internet Control Messages Protocol (ICMP) ECHO packets. Since the destination IP address of each packet is the broadcast address of your network, the router will send a copy of the packet to each host on the network, generating great traffic. If the attacker chooses to spoof the source IP address of the ICMP echo packets, the resulting traffic will not only clog up the originating network and the intermediary networks, but also the spoofed source IP address, known as the "victim" network [**4**].
4. **SYN Attack**:

The SYN Attack is executed during the three-way handshake that kicks off the conversation between two applications over the Internet (**Figure 1**). In this process, the attacker sends multiple TCP SYN packets to a victim requesting to establish a series of connections. For each TCP SYN request received, the victim issues a SYN/ACK response and then places the connection request in a queue. Once the client sends the ACK packet, the victim completes the connection and takes the request off the queue. However, in this case, the client or attacker never receives the corresponding ACK packet, so the requests for connection remain in the queue until the available space is filled up, causing the system to reject any new legitimate requests for communication [**2**].

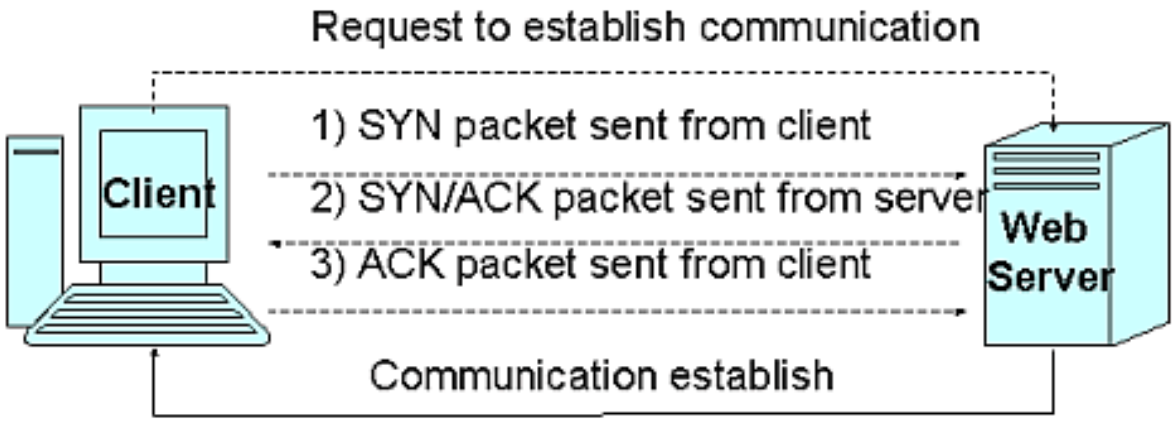

Figure 1: TCP/IP Three-way handshake.

5. **User Datagram Protocol (UDP) Flood Attack:**
   In a UDP connection, a UPD character generation ("chargen") service generates a series of characters for every packet it receives for testing purposes. An attacker can use spoofing to hook up one system's UPD chargen service with another system's UDP echo service, which echoes any character it receives in an attempt to test the network. Therefore, a loop that generates a constant stream of useless packets that clog both systems networks is created [**1**].

DOS Attack Model Development: A Corporate Structure Analogy

As we mentioned before, our attacker starts with the traditional DOS attack model wherein he, the only employee in the company, has to execute each attack directly. As his efforts progress, the attacker's resources and profits increase. With this growth comes the hiring of new employees and managers as he works to realize his plans to become the CEO of his own successful company. More business eventually results in the need to outsource some of the work to maintain a profitable operation. **Table 1** describes the equivalence between the terms used in this scenario and those used to describe the transformations of the DOS Attack model.

	DOS Model	Corporate Structure
Positions	Attacker Slave Master Reflector	CEO Employee Manager Contractor
Goals	Damages	Profits
Needs	Computational Power	Resources

Table 1: Equivalence of DOS Model elements to Corporate Structure elements

DOS Model Development

In **Figure 2**, we have sectioned the DOS attack model development into three stages, each of which represents a transformation from the previous stage by the inclusion of a new element that increases the attacker's computational power. We will explore each of these transformations using the scenario described earlier.

The first transformation (**Figure 2A**) brought the inclusion of slaves into the DOS model. In this case we can think of the attacker as partially successful, and being able to move to a managing position as he hires new employees (equivalent of *slaves*) that will now be in charge of performing the attacks on command. The second transformation (**Figure 2B**) brought in another new element to the DOS model, the masters. Because of the distributed nature of the DOS model at this point, the attack became known as Distributed DOS Attack or DDOS [**6**]. In this case, we think of the attacker as moving to a CEO position, and hiring managers (equivalent of *masters*) to supervise the attacks launched by employees on command, and to cover his tracks after the attacks are completed to avoid trace back.

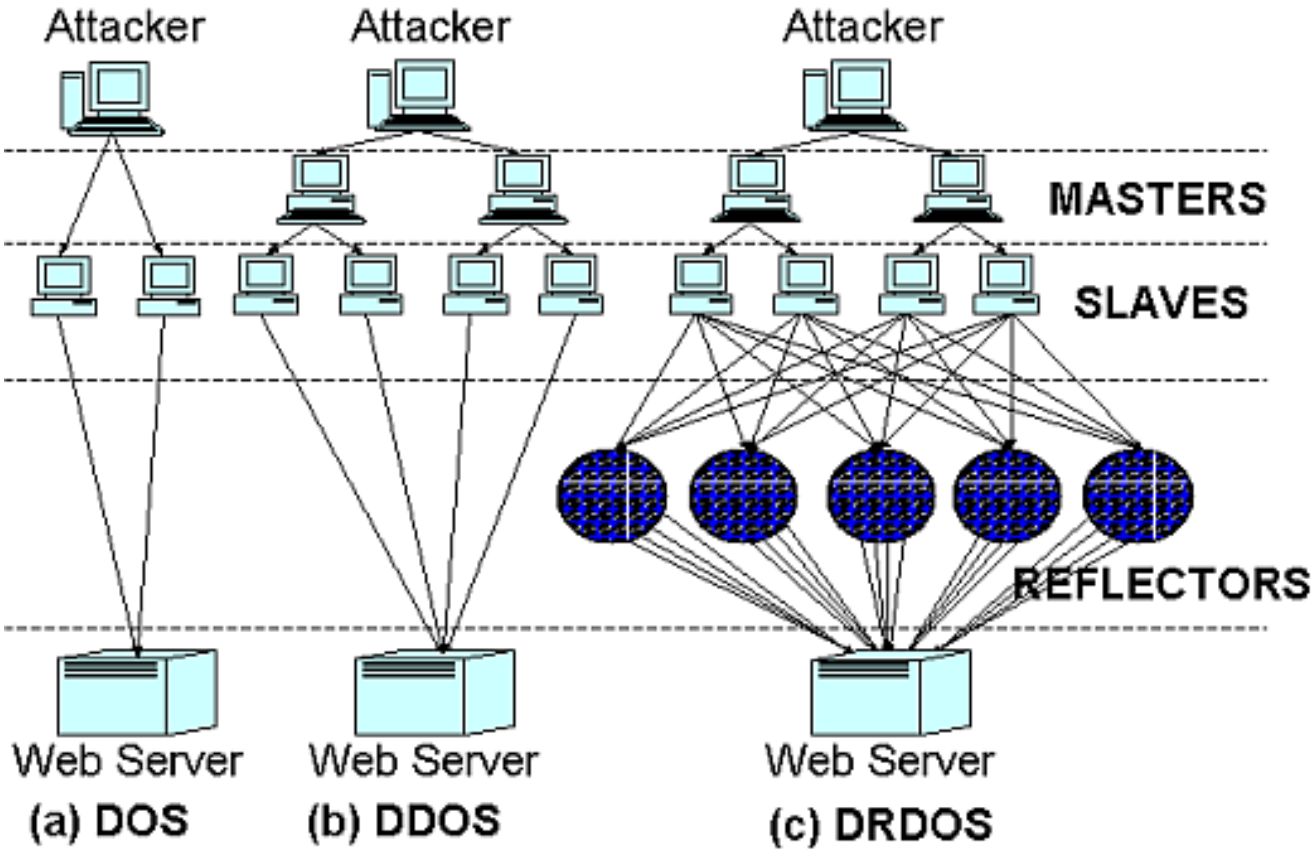

Figure 2: (A) Denial of Service (DOS) Attack, **(B)** Distributed DOS (DDOS), **(C)** Distributed DOS with Reflectors (DRDOS)

The third and most dangerous transformation of the DOS attack model (**Figure 2C**) is known as Distributed DOS with Reflectors or DRDOS [**7**]. As can be derived from the name, reflectors are the new element included in the model at this stage. The inclusion of this element differs in nature from the previous two. Instead of providing more computational power for the attacker, reflectors make it possible to execute a more effective and secure attack, therefore increasing the damages and decreasing the risk of trace back.

We can think of the volume of customers of the attacker's company increasing to such a point as to make it necessary for the attacker to outsource some of the work in order to maintain a profitable operation. The task being outsourced in this case would be the covering of tracks, which now becomes the job of the contractors (equivalent of reflectors). The reflectors' goal is to deflect any response to the attack onto themselves, which is accomplished by having the slaves list a reflector as the originator of the traffic instead of themselves. This DOS model allows the slaves to be free to attack at all times, and also decreases the possibility of trace back since the target server will assume the reflectors to be the originators of traffic, and thus forward all responses to them.

Conclusion

In 2002, our attacker's company made between $1000 and $50 million, which are the lowest and highest amounts of reported financial losses due to DOS attacks in 2002 [8]. As we walk through our scenario, we saw evidence of a rapid increase of computational power of an attacker, as the DOS attack model morphed from DOS to DRDOS. Each transformation can be related to an increase in financial losses from an annual average of $2 million in 1998 to $18 million in 2002 [8], for an average growth of $4 million a year.

Statistics show that DOS attacks are not to be treated lightly. They are a real threat to businesses in today's cyber world, and they become more powerful every day. In April 2000, the National Infrastructure Protection Center (NIPC) released an alert about the 911 Virus, which erased hard drives and programmed computers to dial 911. In spite of efforts to protect against it, a version of the attack resurfaced in July 2002 with a more alarming result. In this case, the virus targeted WebTV user group boards; reports say that once the infected attachment was opened, the WebTV device shut down, rebooted, and dialed 911 [9].

Cases such as the 911 Virus emphasize the fact that the scope of the impact of a DOS Attack can expand beyond the electronic world. With more of our critical infrastructures dependent on networks, a possible combination of physical and cyber-attacks can have a potentially devastating cost in not only money but also human lives. Such might have been the case of the 911 Virus, since its massive spread might have caused a massive DOS attack on the 911 emergency services, delaying or potentially denying access to people with real emergencies.

Corporate growth and financial losses are two fairly familiar terms in today's world. In this article, we matched the development of a corporation to that of the DOS attack model, and furthermore we have related the financial growth of such a corporation to the increase in damage capabilities of the DOS attack model as it has developed with time. Our scenario serves a visualization technique to provide readers with a better understanding of the significance of each of the transformation of the DOS Attack model. The goal was to provide a reference point to the seriousness of the threat that DOS attacks constitute in our system and the potential impact they can have, not only in terms of financial losses, but also in human lives, as described with the 911 virus example. Raising the level of awareness in the business community, as well as in users in general, is the first step toward developing more effective defenses against DOS attacks.

References

1

CERT® Advisory CA-1996-01 UDP Port Denial-of-Service Attack. February 1996 <**http://www.cert.org/advisories/CA-1996-01.html**>.

2

CERT® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks. November 2000 <http://www.cert.org/advisories/CA-1996-21.html>.

3

CERT® Advisory CA-1996-26 Denial-of-Service Attack via ping. December 1996 <http://www.cert.org/advisories/CA-1996-26.html>.

4

CERT® Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks. January 1998 <http://www.cert.org/advisories/CA-1998-01.html>.

5

Huang, C.T. *Denial of Service Attacks.* November 1999 <http://www.cs.utexas.edu/users/chuang/dos.html>.

6

Kessler, Gary C. *Defense Against Distribute Denial of Service Attacks.* Sans Institute. November 29, 2000 <http://rr.sans.org/threats/DdoS.php>.

7

Paxson, Vern. *An Analysis of Using Reflector for Distributed Denial-of-Service Attacks.* Computer Communication Review 31(3), July 2001.

8

Power, Robert. *2002 CSI/FBI Computer Crime and Security Survey.* Computer Security Issues and Trends Vol. VIII, 1, Spring 2002.

9

Worley, Becky. *Virus Dials 911: Police Show Up only to Find Infected WebTV.* abcNews.com, July 2002 <http://abcnews.go.com/sections/scitech/TechTV/techtv_911virus020723.html>.

Biography

Yanet Manzano (manzanof@worldnet.att.net) received her BS in Computer Science from Florida State University (FSU) in 2001. In 2002, she was accepted into the Master's program at FSU, where she is currently a second year graduate student in Information Assurance and Security with the Department of Computer Science. Yanet's research is mainly in computer and network security, especially computer and network forensics, deception technology, security policies, and hacking. During the summer of 2002, she did a professional internship with the Harris Corporation, where she had the opportunity to put her research into practice along with expanding her research interests to include security standards. During the summer of 2003, she continued her internship with the Harris Corporation, and will return to school on the fall to complete her Master's degree in the spring of 2004.