# Denial of service :

Yamina Guenez[1]

[1] Mathematics & Computer Science departement
yaminaguenez@gmail.com
{Guenez, LNCS}@Springer.de
http://www.springer.de/comp/lncs/index.html

**ABSTRACT.** Denial of service (DoS) attacks have become a major threat to curent computer networks. To have a better understanding on DoS attacks,in this paper we have the purpose to present the main types of denial of service (DoS) attacks. Recent years have seen a sharp increase in the number of such attacks.
DoS attacks are classified according to their major attack characteristics. Current counterattack technologies are also reviewed, including major defense products in deployment and representative defense approaches in research.

**Key Words**. DoS, DDoS, Internet Security, Attacks,Teardrop, ICMP Smurfing.

## 1 Introduction

Denial of service (DoS) attacks have become a major threat to current computer networks., this type of attack is used to deny legitimate users access to a resource such as accessing a website, network, emails, etc. or making it extremely slow. Known DoS attacks in the Internet generally is implemented by hitting the target resource such as a web server with too many requests at the same time. conquer the target by exhausting its resources, that can be anything related to network computing and service performance, such as link bandwidth, TCP connection buffers, service buffer, CPU cycles, etc. it is difficult for attackers to overload the target's resource from a single computer, many recent DoS attacks were launched via a large number of distributed attacking hosts in the Internet ,These attacks are called DDoS[1] attacks. It uses a large numbers of compromised computers, as well as other electronic devices such as webcams and smart televisions that make up the ever-increasing Internet of Things to force the shutdown of the targeted network. In this article, we will provide an overview on existing DoS attacks and major defense technologies.

[1] Distributed Denial of Service

## 2 History & State of the Art

Since the first DoS attack that was launched in 1974 by David Dennis who started this attack on his own ,other attacks happend During the mid to late 1990s. DDoS and other DoS attacks have remained among the most persistent and damaging cyber-attacks. These attacks reflect hackers frustratingly high levels of tenacity and creativity and create complex and dynamic challenges for anyone responsible for cyber security.

When IRC[2] was first becoming popular,hackers attempted to force users within a channel to all log out, so they enter the channel alone and gain administrator privileges as the only user present.

Hacking used to require a distinct set of skills and capabilities. These days, DDoS attack services are bought and sold via marketplaces on the Clearnet and Darknet a phenomenon that is closing the gap between skilled and amateur hackers and fueling an exponential increase in threats.

Most of the works presented in books are particularly interested in solutions and protection against these DoS attacks in the network.

## 3 Classification

The variety of DoS attacks are sprouting in the computing world. The major types include Bandwidth based and resource based attacks. Both types consume the entire bandwidth and resources of the network that’s been exploited.Through the analysis made, taxonomy has been depicted in the Fig.1. Depending upon the exploited vulnerability it can be further divided into different types.[3]

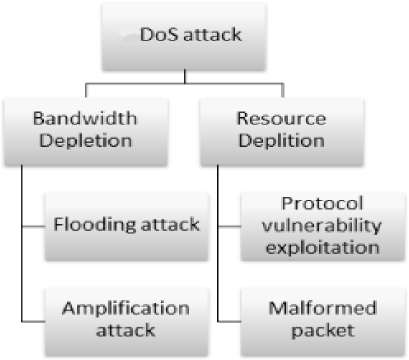

**Fig.1.** Taxonomy of DoS Attacks

[2] Internet Relay Chat

[3] Rashmi V. Deshmukh and Kailas K. Devadkar / Procedia Computer Science 49 ( 2015 ) 202 – 210

## 4 Material & Method

Some techniques allow us to discover attacks and protect users against hackers. But for computer scientists, it is necessary to know the architectures and scenarios of these kind of attacks.

Many attack techniques can be used for DoS purpose as long as they can disable service, or down grade service performance by exhausting resources for providing services. Although it is impossible to enumerate all existing attack techniques, we tried in this section to describe two of them , the "Buffer Overflow" and " ICMP Smurf ing" thechniques.

## 5 Experimental Study

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service, Like :

- attempts to "flood" a network, thereby preventing legitimate network traffic.
- Attempt to disrupt a server by sending more requests than it can possibly handle, thereby preventing access to a service.
- attempts to prevent a particular individual from accessing a service.
- attempts to disrupt service to a specific system or person.

The realization of a DOS is not very complicated, but no less effective. It is possible to attack any type of network equipment.This affects 99% of the world because most denials of service exploit vulnerabilities related to TCP / IP[4].

### 5.1 Types Of attacks :

#### 5.1.1 ICMP Smurfing

ICMP[5] Smurf Flooding. ICMP known as a Ping flood attack, is a common Denial-of-Service (DoS) attack in which an attacker attempts to overwhelm a targeted device with ICMP echo-requests (pings). In a smurf attack, attacking hosts forge ICMP echo requests having the victim's address as the source address and the broadcast address of these remote networks as the destination address (CERT 1998). As depicted in Figure 1, if the firewall or router of the remote network does not filter the special 6/28 crafted packets, they will be delivered (broadcast) to all computers on that network. These computers will then send ICMP echo reply packets back to the source (i.e., the victim) carried in the request packets. The victim's network is thus congested.

[4] the Transmission Control **Protocol**/Internet **Protocol**, is a suite of communication **protocols** used to interconnect network devices on the internet.

[5] Internet Control Message Protocol

Attacks can be separated into three categories, determined by the target and how the IP address is resolved:

- Targeted local disclosed – In this type of attack, a ping flood targets a specific computer on a local network. In this case, the attacker must obtain the IP address of the destination beforehand.
- Router disclosed – Here, a ping flood targets routers with the objective of interrupting communications between computers on a network. In this type of attack, the attacker must have the internal IP address of a local router.
- Blind ping – This involves using an external program to reveal the IP address of the target computer or router before launching an attack.

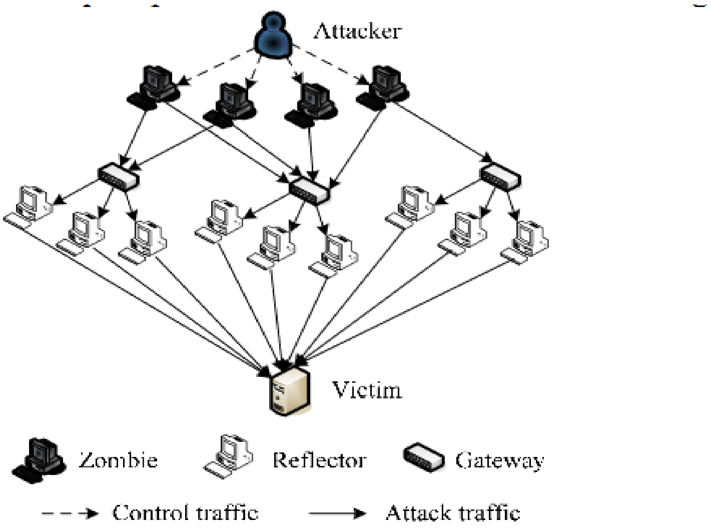

**Fig.1.**ICMP Smurf Attack

### Consequences of ICMP smurf Attack

The damaging effect is directly proportional to the number of requests made to the targeted server. Unlike reflection-based DDoS attacks like NTP[6] amplification and DNS[7] amplification, this type of  attack traffic is symmetrical; the amount of bandwidth the targeted device receives is simply the sum of the total traffic sent from each device.

[6] Network Time Protocol amplification  is a type of  DDoS attack in which the attacker exploits publically-accessible  NTP servers to overwhelm the targeted with User Datagram Protocol (UDP) traffic.

[7] domain name system  amplification is a reflection-based DDos attack. The attacker spoofs look-up requests to DNS servers to hide the source of the exploit and direct the response to the target.

**How is a ICMP Smurf Attack mitigated?**

Disabling a ping flood is most easily accomplished by disabling the ICMP functionality of the targeted router, computer or other device. A network administrator can access the administrative interface of the device and disable its ability to send and receive any requests using the ICMP, effectively eliminating both the processing of the request and the Echo Reply. The consequence of this is that all network activities that involve ICMP are disabled, making the device unresponsive to ping requests, traceroute requests, and other network activities.

### 5.1.2 Teardrop Attack

is a DoS attack that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, One of the fields in an IP header is the "offset" field, indicating the starting position, of the data contained in a fragmented packet relative to the data in the original packet. If the sum of the offset and size of one fragmented packet differs from that of the next fragmented packet, the packets overlap. When this happens, a server vulnerable to teardrop attacks is unable to reassemble the packets - resulting in a denial-of-service condition.

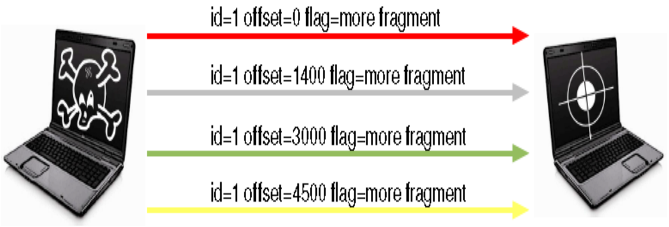
id=1 offset=0 flag=more fragment
id=1 offset=1400 flag=more fragment
id=1 offset=3000 flag=more fragment
id=1 offset=4500 flag=more fragment

**Fig. 1.** Sending a fragmented package

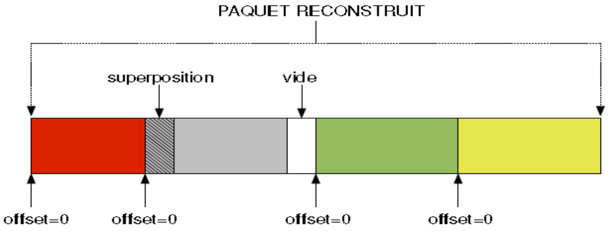

**Fig. 2.** Reception and reconstruction of the package

**Consequences of the Teardrop Attack**

- block the TCP / IP service, System lock , Crash system , Reboot system.

**How is a Teardrop Attack mitigated?**

-Update the operating system &packet management in the implementation of tcp/ip.

## 6 Importance & Impact

Depending on the impact of a DoS attack on the victim, the attacks are classified as disruptive and degrading attacks. So we see more and more attacks that are targeted representing a new blackmail technique that good numbers of pirates now exercise blithely. Indeed, Cutting off some business from the internet can lead to significant loss of business or money. The internet and computer networks power a lot of businesses. Some organizations such as payment gateways, e-commerce sites entirely depend on the internet to do business, are now all threatened.

Current hackers are therefore using denial-of-service attacks as a new weapon to blackmail companies connected to the Internet. It is obvious that the slowing down, or even the blocking of their services for a few hours, could result big losses of money as well as a lot of inconvenience for their customers. These companies have every interest in obeying or finding a way to protect themselves.

This new weapon is now used more and more commonly. Any internet accessible company is open is potentially at risk. Note also the number of attacks of this kind increases each year.

## 7 Conclusion

we overviewed existing DoS attacks and defense technologies in the Internet. DoS attackers exploit flaws in protocols and systems to deny access of target services. Attackers also control a large number of compromised hosts to launch DDoS attacks. Simply securing servers are no longer enough to make service available under attack, since DoS attack techniques are more complicated and many unwitting hosts are involved in DoS attacks.

Some solutions can handle some but not all DoS attacks due to their design principles, deployment issues, etc. To protect against this type of attack, it is necessary to invest in internal security by creating a dedicated position or service within the company.

## References

1. Denial of Service Attacks Qijun Gu :
   https://s2.ist.psu.edu/ist451/DDoS-Chap-Gu-June-07.pdf
2. Dos attack Tutorial Guide :
   https://www.guru99.com/ultimate-guide-to-dos-attacks.html