



FIST Conference October 2004

Denial Of Service Attacks

© Gabriel Verdejo Alvarez (gaby@tau.uab.es)

Barcelona



INDEX

Speaker's introduction.

Denial Of Service attacks (DOS).

Examples.

Distributed Denial of Service attacks (DDOS).

DDOS tools analysis.

Reflection DDOS Attack.

Countermeasures.

What the future brings.

Questions.

Bibliography.



Speaker's Introduction

Gabriel Verdejo Alvarez, Barcelona 1973.

Computer science engineer at UAB.

PhD studies (DEA) at CCD department, UAB.

Senior consultant over 5 years experience.

Cisco Certified teacher (CNAP).

Since 2002 working at LSI department located at UPC.



Denial Of service attacks I

Historical context:

90's decade became the Internet age (WWW).
Massive deployment of part-time connections (modem).
Bandwidth increase → Interaction, pictures...
A new mass media has born!

Hackers context:

Simple attacks techniques (console VT, dial-out War games...)
Almost inexistent networks attacks (IRC Wars).



Denial Of service attacks II

A brief chronology:

Until 1996 naive attacks. No worldwide connection available.

1997 TRIN00 tool became the starting point of Denial Of Service attacks.

1988 TFN tool improve DOS attacks.

1998 Ebay, Yahoo, Microsoft were the favorite targets for this kind of attacks.

1999 TFN2K the new generation for denial attacks.



Denial Of service attacks III

Definitions:

Denial Of Service (DOS) means the impossibility of getting access to a resource or service by the legitimate user.

Denial Of Service attack is when the resource or the service is monopolized intentionally to prevent access from other users.

This definition also includes the attempts to collapse the service or resource to deny access to anyone.



Denial Of service attacks IV

DOS attack example 1: **IP Flooding**

Used in local networks → Consumes great amount of bandwidth.

The attacker creates spurious traffic over the network:

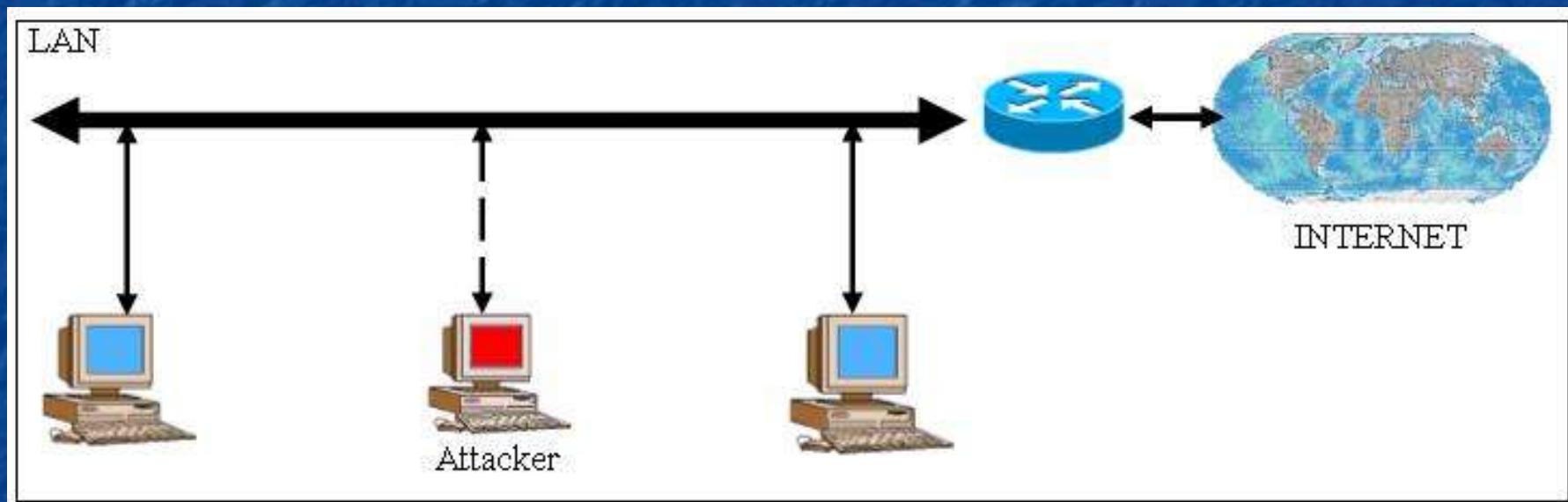
Random

Guided

Traffic can be UDP, ICMP or TCP.



Denial Of service attacks V





Denial Of service attacks VI

DOS attack example 2: **ECHO-CHARGEN / Snork**

UNIX computers provides several well known services (Telnet, FTP, ECHO...).

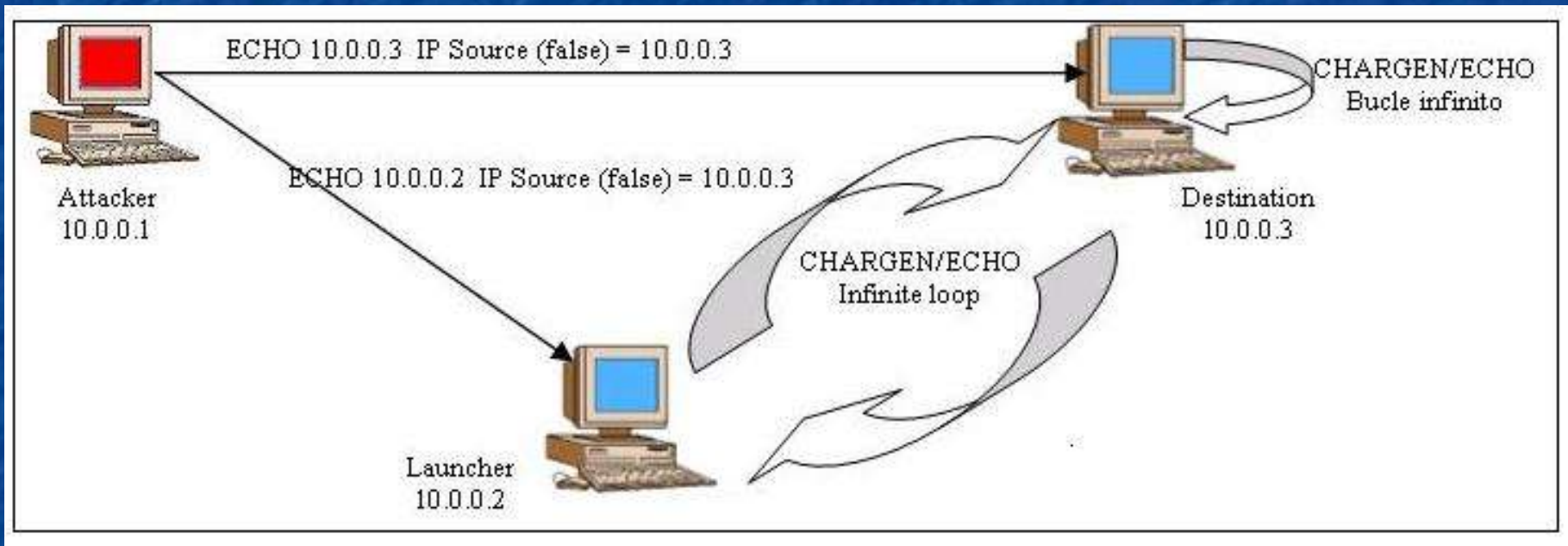
ECHO: Replies any PING request received over the network.

CHARGEN: Replies any network request with a random character generator.

The attacker spoof the source address of the request crossing both services.



Denial Of service attacks VII





Denial Of service attacks VIII

DOS attack example 3: **Ping Of Death**

The most famous DOS attack.

Uses programming bugs and RFC791/RFC792 definitions of maximum packet length of TCP/IP family:

IP datagram has a maximum size of 64K (65535 bytes) with a typical header length of 20 bytes.

ICMP packet is encapsulated into IP datagram and has a 8 bytes header.



Denial Of service attacks IX

Attacker "can" send 65510 bytes of data using ICMP protocol because:

$$65535 - 8 \text{ (header)} = 65527 \text{ bytes}$$

The destination computer receives the request and tries to reassemble data:

But the truth is we have $65535 - 20 - 8 = \mathbf{65507}$ bytes free!!

This attack causes overflow in networks services or operative system failure.



Distributed Denial Of service attacks I

Definitions:

Distributed Denial Of Service Attacks (DDOS) can be defined as a deny of service attack with several sources distributed along the Internet that focuses on the same target.

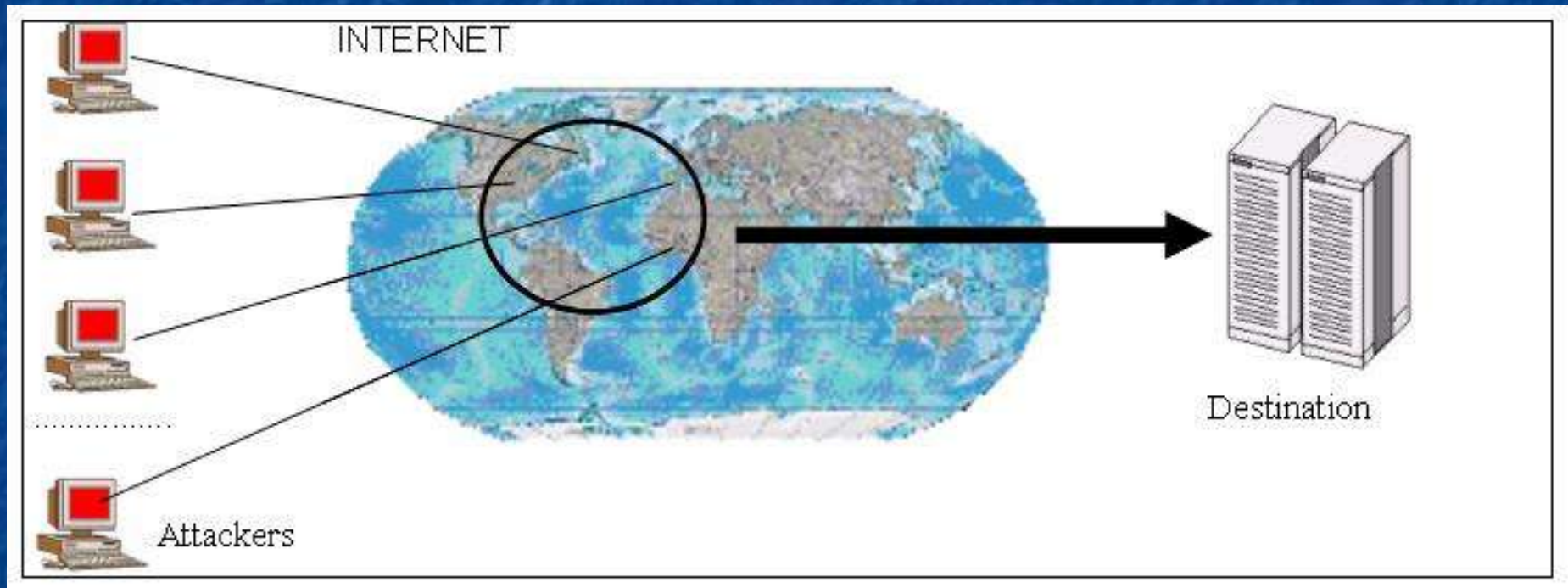
Unlimited number of sources can be used.

Worldwide distribution.

Any computer attached on Internet can be disabled.



Distributed Denial Of service attacks II





Distributed Denial Of service attacks III

DDOS tools analysis: **TRINOO** / **TRINOO**

First DDOS tool find "in the wild". Originally detected in Solaris machines but could be used in any UNIX computer.

The deployment mode follows always these guidelines:

The hacker goes into the computer (bugs exploit...).

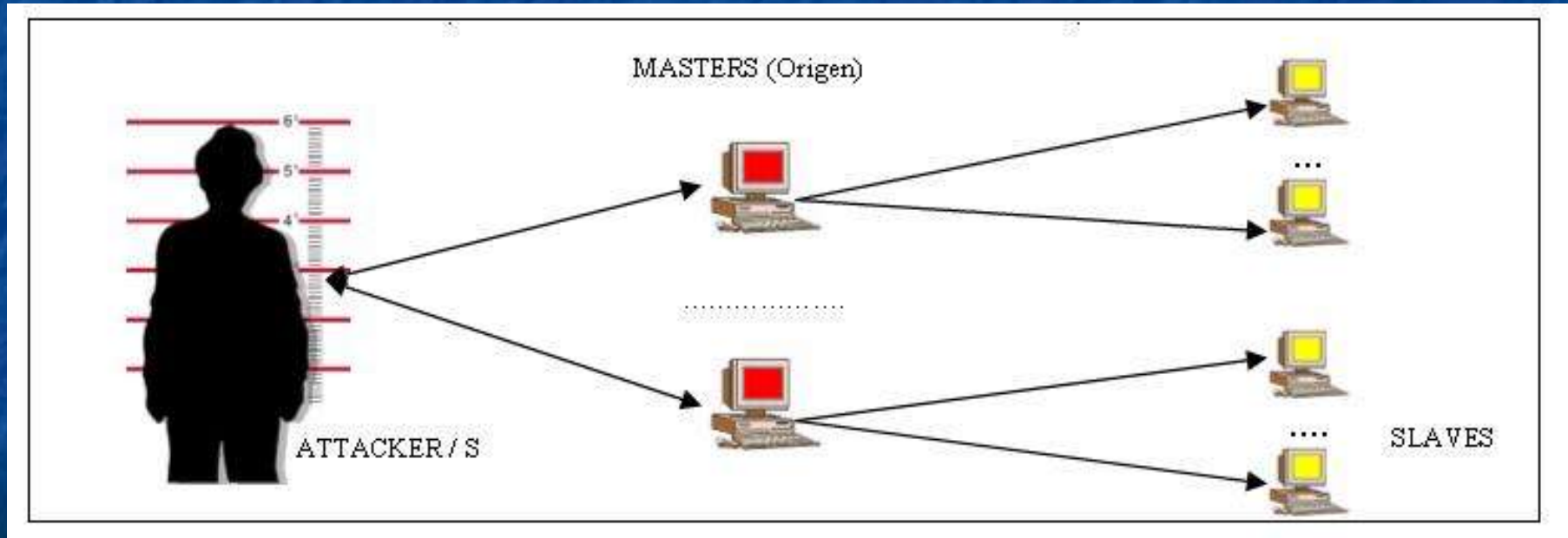
Software is **compiled** leaving a backdoor at port 1524/TCP.

Other machines in the same network are hacked.



Distributed Denial Of service attacks IV

Implements a hierarchical model based on a master-slave schema to permit the DDOS attacks.





Distributed Denial Of service attacks V

A single attacker can control hundreds (even thousands) of machines in a very simple way.

The attacker cannot be identified directly (the attacker computers are the slaves!).

This tool implements IP flooding attack.

The daemon lets the user run several commands (Telnet style) to start/stop service and to control the beginning and the end of every attack.



Distributed Denial Of service attacks VI

DDOS tools analysis: **TFN2K**

The most sophisticated tool find in the wild.

Improves communication between master/slaves computers using TCP, UDP or ICMP packets (even all!!) to avoid firewalls / IDS.

Implements different styles of attacks (TCP/UDP/ICMP flood, Smurf) that can be automatically rotated to avoid basic countermeasures.



Distributed Denial Of service attacks VII

Packet headers are randomly changed to prevent IDS signatures.

Daemons do not reply to the orders they receive. Every command is resend 20 times. This method make difficult to discover compromised computers because no outside communication exists.

Uses CAST-256 as cipher method to prevent the sniffer tools over the network.



Distributed Denial Of service attacks VIII

Reflection DDOS attack:

This new approach is based on the use of legitimate (not hacked!) computers attached to the Internet.

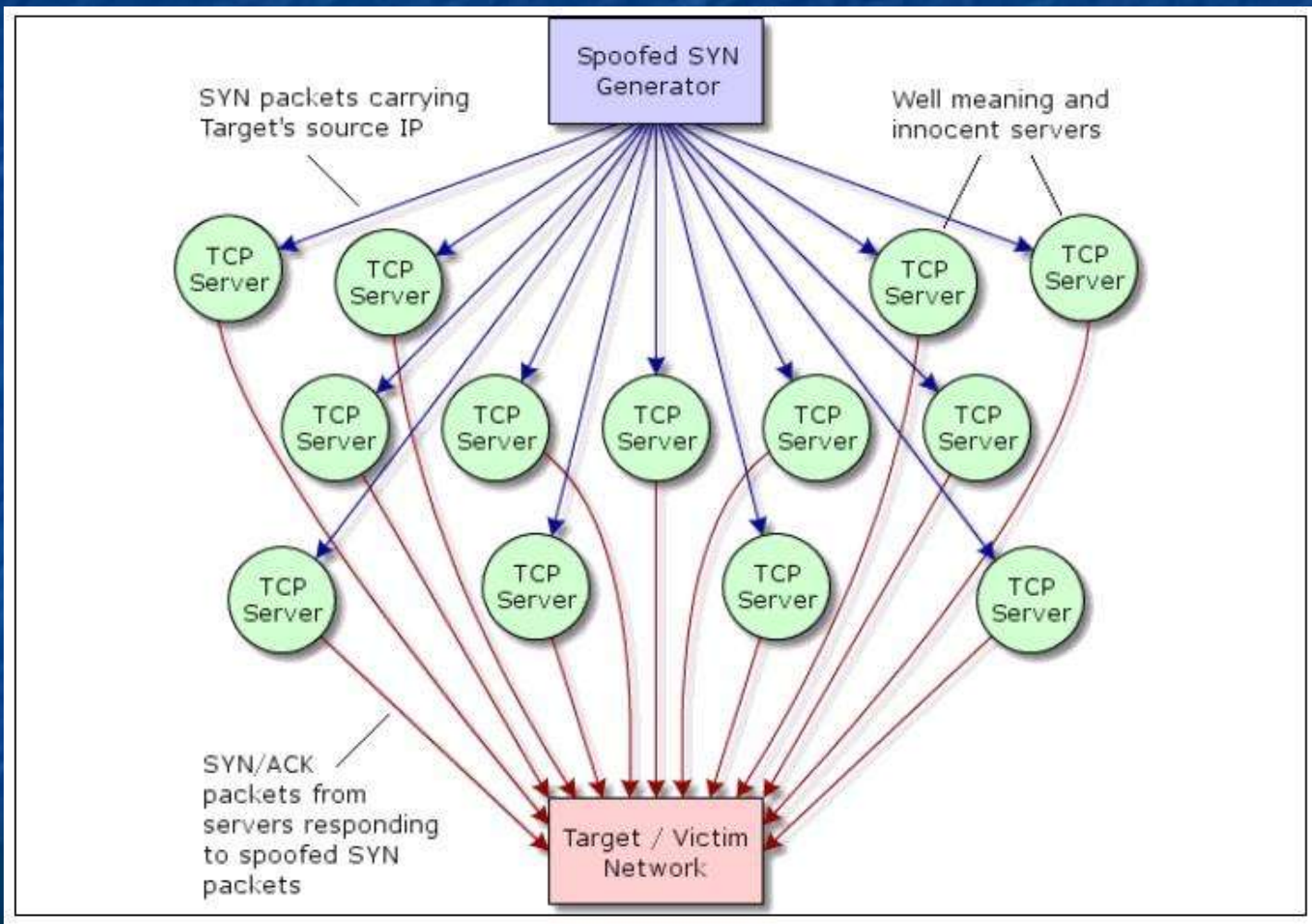
The slaves machines are not quickly discovered/banned so the attack can be done more time.

The attacking method can be switched automatically.

The "attackers" computers can change without randomly make more difficult the detection of the attack.



Distributed Denial Of service attacks IX





Distributed Denial Of service attacks X

GRC.com DDOS reflection attack:

On January 11 of 2002 an attack to GRC was discovered.

2 x T1 connection were collapsed few hours by several ISP computers as Verio or Qwest and well known places as Yahoo.

Few hours before it was detected a filter was applied and the count of packets discarded were **1.072.519.399!!!**



Distributed Denial Of service attacks XI

Countermeasures:

Ingress/Egress filtering → Deny spoofing address attacks.

Firewalls → Poor solution, increases routing overhead.

IDS → Bad detection mechanism and limited response.

Other solutions (Multops, Reverse Firewall, D-Ward) cannot interoperate with external systems.



Distributed Denial Of service attacks XII

What the future brings:

The DDOS problem is not solved and periodically we read a new successful attack against any major company (Ebay, SCO...).

The future of DDOS are changing with virus symbiosis. Now the hacker does not need to enter into the computer, the virus let the door open.

MyDoom (2004) www.sco.com → www.thescogroup.com

DDOS attacks in wireless Networks.



Distributed Denial Of service attacks XIII

Bibliography:

William R. Cheswick and Steven M. Bellovin, "Firewalls and Internet Security: Repelling the Wily Hacker", Addison-Wesley Publishing, 1994.

W. Richard Stevens, "TCP/IP Illustrated Volume 1: The protocols", Addison-Wesley, 1998.

David Dittrich, "The TRIBE FLOOD NETWORK distributed denial of service attack tool", 1999.

David Hoelzer, "Intrusion Detection FAQ: Why Egress Filtering Can Benefit Your Organization", 2000.

T. M. Gil, M. Poletto, "MULTOPS: a data-structure for bandwidth attack detection", 10th Usenix Security Symposium, 2001.

<http://tau.uab.es/~gaby> gaby@tau.uab.es