

Arabic Academy For Banking And Finance  
Computer Information System Dept.

Damascus, 2006/2007.



## Internet Worm Propagation Modeling & Simulation

Presented by

Eng: Fadi BAGHDADLIAN

# Abstract

Have you ever tried to use the phone on a special occasion like New Year or mother day? Did you face some problem in making the call? If yes then you know the distributed denial of service, it happens when the number of users trying to use a service is bigger than the capacity of the service provider.

In the phone call example, let us assume that the telephone network can serve 1000 users in the same time; normally less than 1000 user will use the network at the same time, but in some special occasion more than 1000 users may use the network and that causes Denial of Service (DoS) for many users.

In computer network we have the same idea, if the number of clients that try to connect to a Server is bigger than the band width of the Server then we will face DoS.

Many attackers are using this technique to attack servers on the internet. This threat started with Morris worm 1988 and continued until our days without a solution (Code Red worm – 2001 , SQLSlammer worm – 2003 , MyDoom – 2004 ...)

We will study Internet Worms, and the different approach for modeling their propagation on the internet.

# 1. Introduction

## 1.1 Introduction of Internet

The first attack on the internet was on 1988 with a worm named Morris worm. And this worm changed people's way of thinking towards internet. In the beginning the main concern when connecting to the internet is the connection itself, but after 1988 there is more than the connection to think about... There is Security problems.

Mr. Dave Clark tells a story about an angry manager wondering how the problem of Morris worm could happen. And Dave Clark answers him that this is what the internet was designed to do: spread the worm as quickly and efficiently as possible.

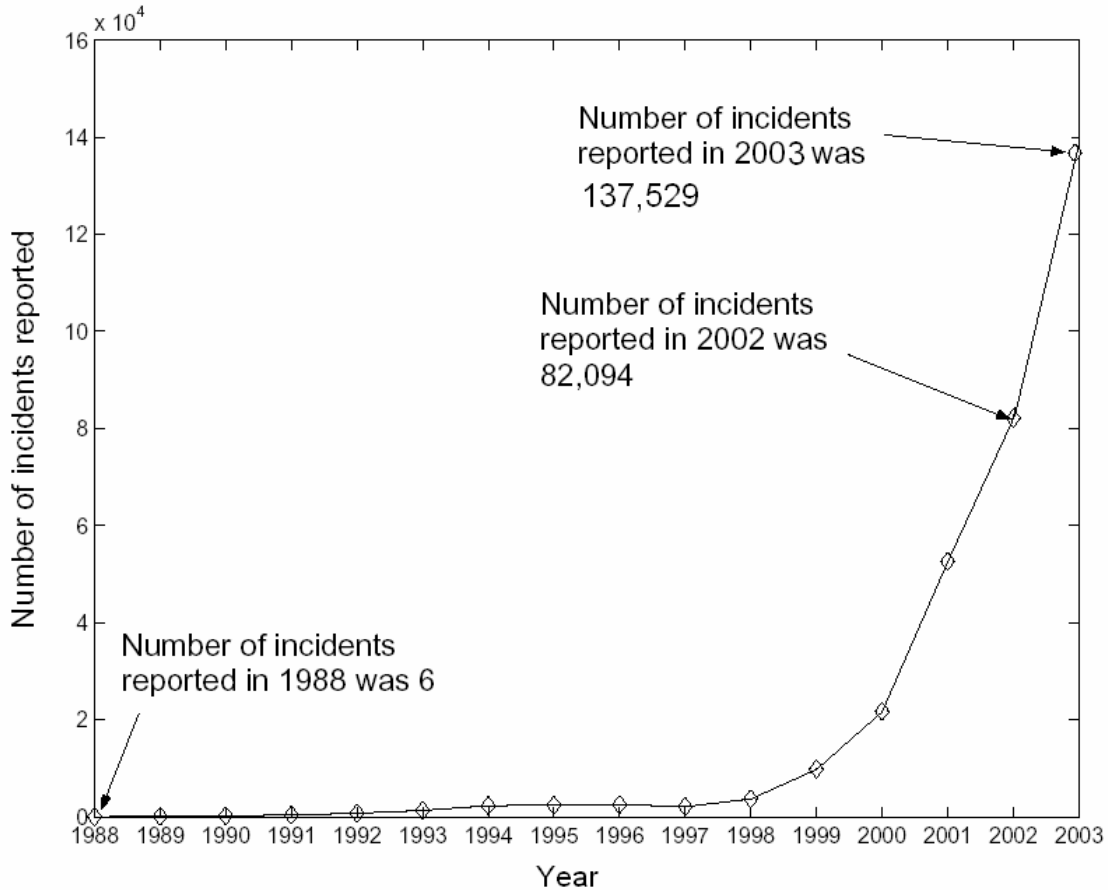
In the beginning there were no problems with Internet since most users were scientists but now every one uses internet and we are facing more and more of cyber crimes. [11]

Now after 18 years we still face the same problems similar to Morris worm Some of the famous attacks were the Code Red and Nimda worms that infected hundred of thousands of computers in 2001. And these worms caused the loss of millions of dollars.

The SQL Slammer worm attack in 2003 was very fast and within 10 minutes more than 90% of vulnerable computers were infected. And it caused denial of service of many networks in Asia, Europe & America for several minutes. This worm was called the first "Warhol" because it was able to stop a big portion of the internet within 15 minutes

The dangerous effects of such worms, provoked many organizations such as" CERT, CAIDA, and SANS Institute" to monitor the internet and to detect any suspicious packets. They analyze all packets to detect any abnormal network activities. These centers are the basis for a future nation worm monitoring and early warning system. [26]

The following chart represents the number of Internet security incidents reported from 1988 to 2003 [8]



Other problem with the internet is DoS, the most famous DDoS attacks in 2000 where some important dotcom sites like yahoo, eBay & Amazon were stopped for 2 days and costed the companies millions of dollars. [24]

Some times the worm spread on the internet very fast and make congestion on routers making DoS attacks and some other times the worm may be programmed to make DoS attack after the spreading phase.

We will study first the denial of service attack then we will present the different approach in modeling worm spreading on the internet.

## **1.2 Background in Computer Threat:**

Since the existence of computers, we faced many threats like: Viruses, Email Viruses, Worms, Trojan horse and Denial of service.

We will introduce these types of threats:

***Virus:*** Computer program that spreads by inserting copies of itself into other executable code or documents; it is similar to the biological virus which spreads in a live cell. Some types of the virus attack disk boot sectors. Some others just attack exe or com files. Usually they have a logical or timing bomb where the virus will attack its victim.

***E-mail viruses:*** it is a type of virus that uses an e-mail message as a mode of transport, and it automatically emails itself to all email addresses found in the victim's address book. One of the famed is "Mellisa"

***Trojan horses:*** it's a computer program pretends to do one thing such as compressing files while it is damaging them.

***Worms:*** it's a piece of software that uses computer networks and security flaws to create copies of itself. A copy of the worm will scan the network for any other machine that has a specific security flaw. It replicates itself to the new machine using the security flaw, and the replicating process continues. There are many famous worms like "Love Bug worm". Some times the worms cause DoS attack.

Unlike viruses and trojans which rely on human intervention to spread, worms are self-replicating software designed to spread throughout a network on their own.

***DoS:*** Denial of Service is stopping a program or computer or network from working to deny the legitimate user from using the system. And this is the subject of our research... Some experts do not classify the DoS as threats, but as a consequence of other threats like worms.

All the previous threats are called malware (malicious software) that is software designed to make harm to your system. They use a bug in the systems or they flood the systems with traffics to make harm to your system.

### **1.3 Background in Defense [16]**

There are many software and hardware that deal with the previous threats:

**Antivirus:** software that searches for viruses in all files that come to our system. And also searches for the suspicious action that may be caused by unknown virus (like writing on boot sector). The most famous are Semantic and MacAfee antivirus.

**Firewall:** it is a hardware or software that prevents any unauthorized access to our network; it helps in preventing some types of DoS attacks. Well known software firewall included with windows XP (internet connection firewall) and in Hardware firewall the most famous are Cisco Pix firewall.

**Intrusion detection or preventing systems:** it is like a monitor that waits for specific suspicious network traffic, and then it alarms about the incident and sometimes it takes action immediately. Some times the ISD or IPS are included with the firewall.

Many companies produce a single software product that have antivirus, antispam, firewall and IDS in one package like Norton security center.

We split our work into the following tasks:

- General introduction about security
- Study the different types of DoS & DDoS
- Modeling of Worm Propagation
- Conclusion and recommendation

## 2 Study Of DoS

Many network attacks try to gain access to systems and use variety of creative techniques to achieve this goal like sniffing, spoofing & session hijacking.

Other attacks don't care to obtain access; they want only to stop critical services or to prevent legitimate users from access into the system. We call this type of attack Denial of Service attack, and we refer to it as DoS not DOS to distinguish it from Disk operating system.

### 2.1 Classification of DoS [15]

	Stopping Services	Exhausting Resources
Locally	<ul style="list-style-type: none"><li>• Process killing</li><li>• System reconfiguration</li><li>• Process crashing</li></ul>	<ul style="list-style-type: none"><li>• Forking processes to fill the process table</li><li>• Filling up the whole file system</li><li>• Sending many traffic to the outside</li></ul>
Remotely	<ul style="list-style-type: none"><li>• Malformed packet attack</li></ul>	<ul style="list-style-type: none"><li>• Packet floods (Usually DDoS)</li></ul>

#### ***1- Locally Stopping Services:***

If a user has administration privileges, he can shut down any critical services offered by the system, in fact he can shut down all the system!

The hacker can kill important process or can change the system configuration that denies the service indirectly, for example the user can change NAT configuration and deny any external user from accessing a web server.

If the user doesn't have privilege to kill a critical process, he can crash the system using any existing vulnerability like overflow attack.

#### ***2- Locally Exhausting Resource:***

There are many recourses that if exhausted will stop any user from accessing the system. If a user has privileges he can fill in the process table of the file system. If he has no privileges he can send traffics to the outside and that will flood the system and deny any external user from accessing the system.

### **3- Remotely Stopping Services:**

Usually there are many bugs (vulnerabilities) in any system, some of them will cause the system to stop, and if the crackers find these bugs they will use them to make DoS.

### **4- Remotely Exhausting Resource:**

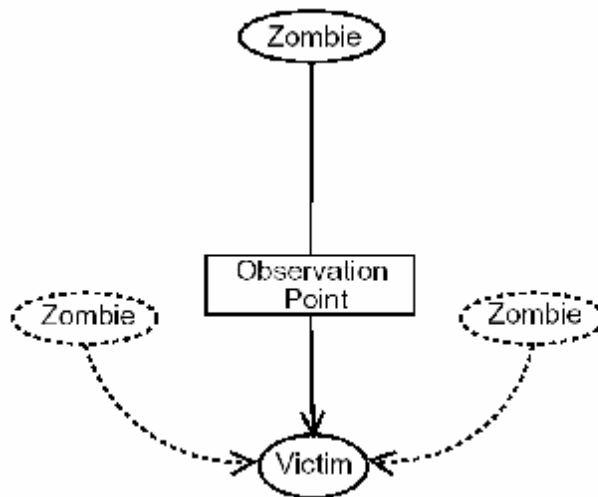
If the cracker doesn't find any vulnerability on the system he will try to exhaust the target resources, like CPU, Buffers & Communication link. For example he floods the server with many packets and the DoS attack will be successful if he has a band width bigger than the band width that the victim can support.

We can also distinguish between 3 types of the Remotely Exhausting Resource:

Based on the location of observation point: [1]

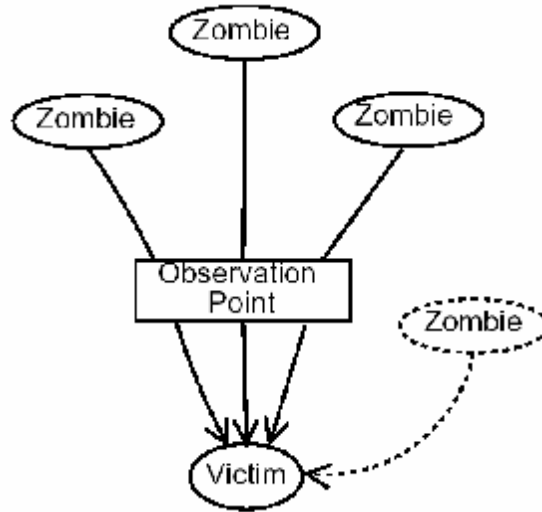
- Single-source:

When a single attacker (Zombie) is flooding the victim



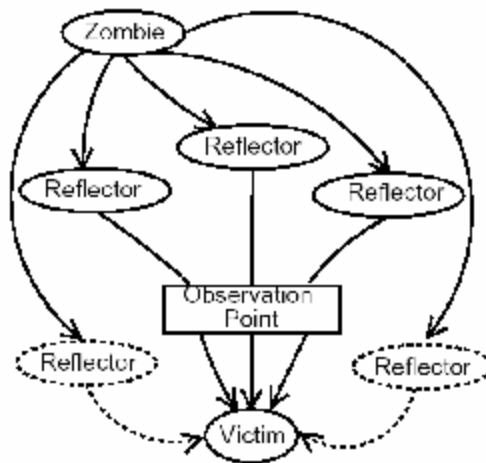
- Multi-source

When multi attackers (Zombie) are flooding the victim



- Reflector

It is a special case of Multi-sources, the attacker tries to hide his identity or to amplify the attack. An example of this attack is sending TCP SYN to a web server (Reflector) with spoofed source IP address (Victim IP), so the SYN-ACK will return to the victim, not to the attacker.



## 2.2 Example of DoS

**1- SYN Flood:** sending flood of TCP/SYN packets usually with a spoofed IP address, each packet is treated as a connection request, these requests cause the server to send TCP/SYN-ACK packet and wait for TCP/ACK that will

never come. If the number of packets is more than the resources available (Timers & memory) the server will stop responding to any real TCP connection.

## **2- ICMP flood**

**2-1 Smurf Attack:** the attacker sends a large number of ICMP echo traffic to the broadcast address and puts the victim address instead of the source address. Then all the machines on the broadcast network will reply to the victim and this consequently will cause DoS.

**2-2 Ping flood :** the sender floods the victim with many ICMP echo packets (ping). This attack will succeed if the attacker's band width is bigger than the victim's.

**3- Fraggle attack (UDP flood):** it is similar to Smurf attack, but the packet is UDP echo instead of ICMP echo.

**4- DNS attack:** this type is similar to Smurf attack; the attacker sends a DNS request to a nameserver with a spoofed source IP address with the Victim address. When the DNS server replies to the request, it replies to the victim instead of the attacker. This is a useful reflector attack, since the DNS reply has large size and can flood the victim.

**5- Buffer overflow:** programming error that may cause exception in memory and program termination or may cause security breach.

**5-1 Ping of Death:** sending a ping with size bigger than the usual size 64 bytes. Many old OS crashes when receiving a ping with the size 65,536.

**5-2 Morris worm:** a worm that exploits a buffer overflow bug in UNIX service called fingerd system (1988).

**5-3 Code Red worm:** a worm that exploits a buffer overflow bug in Microsoft Internet Information Service (IIS) 5.0 (2001).

**5-4 SQLSlammer worm:** a worm that exploits a buffer overflow bug in Microsoft SQL Server 2000 (in 2003).

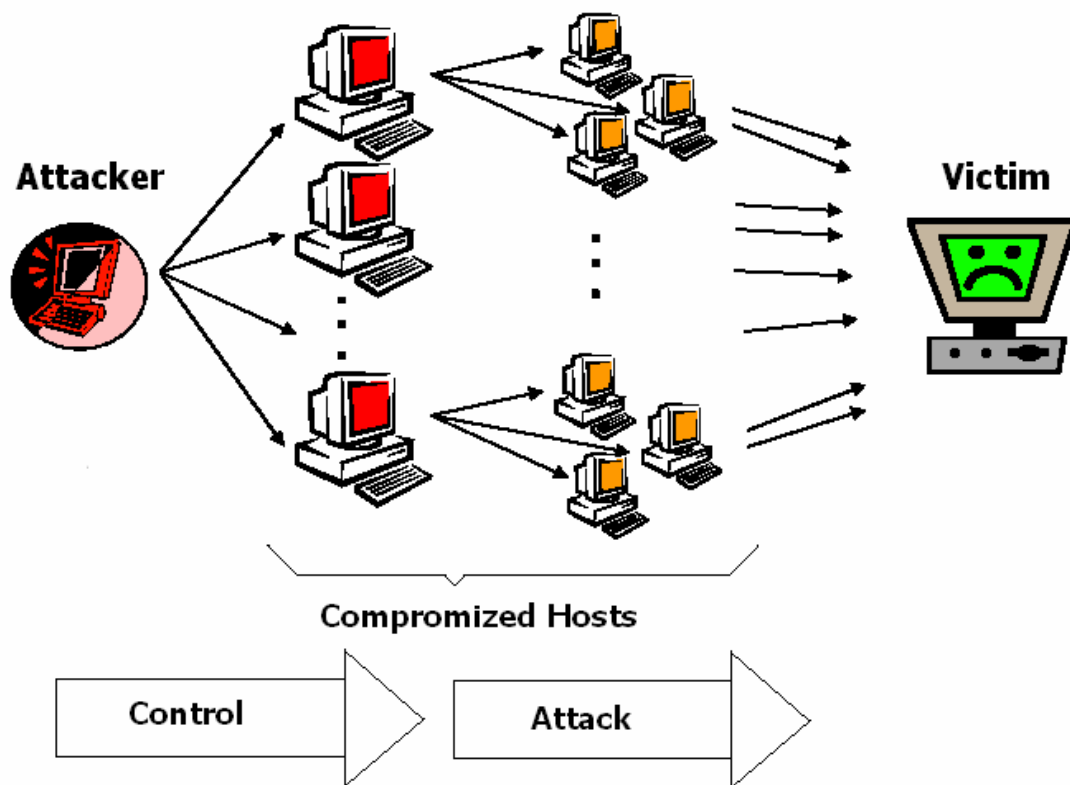
**6- DDoS (Distributed denial of service attack):** more details on the DDoS in the next paragraph.

### 2.3 Definition of DDoS.

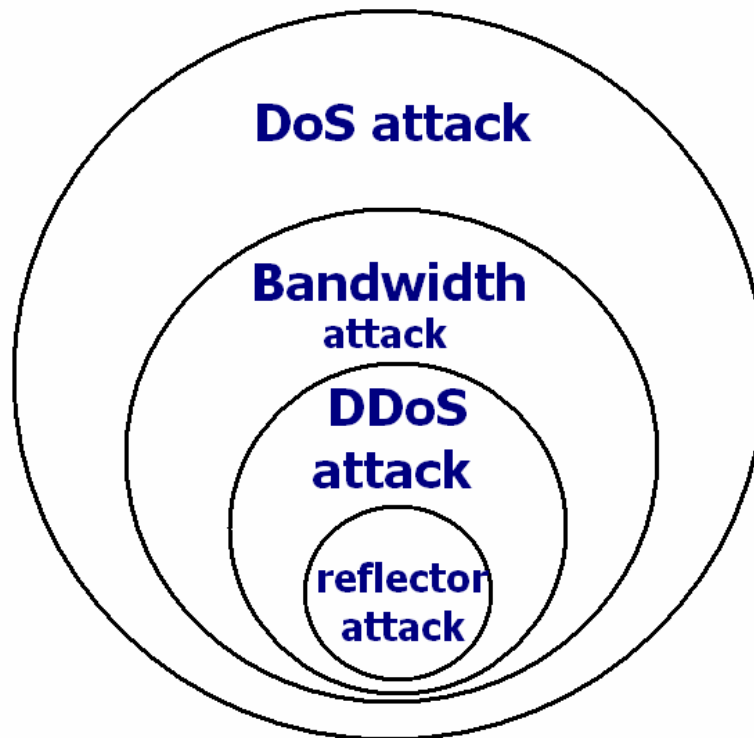
A DDoS attack directs hundreds or even thousands of compromised “zombie” hosts against a single target.

With enough zombies the victim won't be able to answer any legitimate users.

To start a DDoS attack we should have a big laboratory plain of computers that will attack together the victim, or we will use a single computer and a worm that will do the dirty job: spread from host to host and then attack in a specific time.



To understand the relation between DoS and DDoS please see the following picture



The relation of different types of attacks [22]

The bandwidth attack uses single node to attack the victim, and it makes use of some aspects in the protocols like the SYN-ACK problem.

DDoS attack is similar to bandwidth attack except that it uses many nodes to start the attack.

Reflector attack is similar to DDoS attack, except that it uses reflection in the last step near the victim to amplify the attack and to hide its source.

## 2.4 Why DDoS is possible?

The designers of the internet haven't expected that it will be widely adopted and used; they thought that only the scientists will be using this network. That's why they haven't considered thoroughly security issues.

There are many features of internet that make it vulnerable to DDoS attack: [18]

- **Internet security is highly interdependent:** The DDoS attack uses some vulnerable hosts on the internet to launch the attack.
- **Internet control is distributed:** Each host runs according to its network configuration, there is no global configuration for the hosts connected to the internet.

- ***Internet resources are limited:*** any internet host (victim) has a limited resources (memory, band width, CPU) so there will be a number of hosts who have more resources and can attack the victim.
- ***Accountability is not enforced:*** there is no method of identifying the source of any packet, the packet contains its source address but it could be spoofed and this gives the attacker a possibility to escape from accountability for their actions.

# 3 Modeling of Worm Propagation

## 3.1 Introduction:

The big loss caused by worms make the scientist work harder to find a defense against them. They are trying to model them and study their behavior for developing much more robust systems.

## 3.2 Simulation and Alternatives: [6]

We have 4 different ways to study the characteristic of worms:

### 3.2.1 Mathematical Models:

This is the more powerful approach, but it is hard to do or even impossible in some cases.

### 3.2.2 Testbeds:

This method tries to isolate certain hosts and study the worm propagation on them, but the problem is that the new worm spreading use huge amount of hosts.

### 3.2.3 Real World "Experiments":

Since worm writers use the real world, why the scientists could not make experiments on real world? This method is out of question for moral reasons.

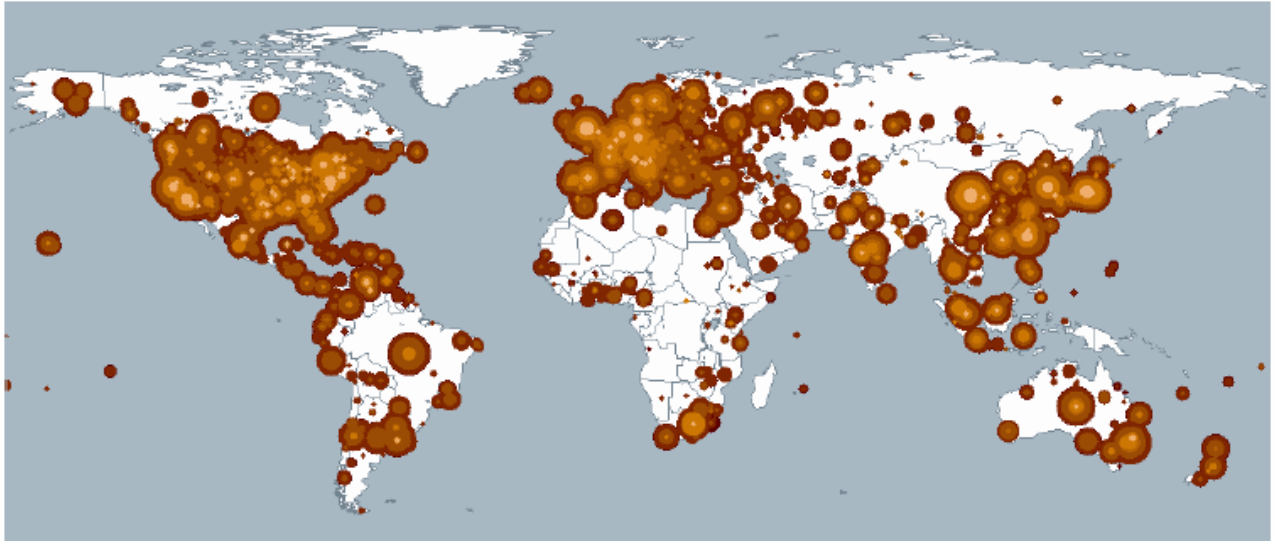
### 3.2.4 Simulation:

This method is very helpful in reducing mathematical complexity.

## 3.3 Study of Worm Example (Code Red):

Code Red was the big shock for computer users since it was the first worm with height propagation rate and causes a loss of 2.6 billion of dollar. It infects about 359.000 hosts in 10 hours.

The following picture show the hosts infected in all over the world: [7]



On June 18<sup>th</sup> 2001 a serious Windows IIS vulnerability was discovered, after one month the first version of Code Red was released, but it did not propagate well because of a bug in its code.

At 10:00 UTC of 19 July, the second version of Code Red was released, it use the vulnerability in Windows IIS and another vulnerability of CISCO routers.

This worm generates 100 threads on the infected machine, and each thread generates random IP address and tries to connect to it. The connection will succeed if it is with a vulnerable Windows 2000 host.

After establishing the connection, the worm will copy itself to the new host and try the same activities from the beginning.

If the connection was not success the thread generate new IP address and try again.

At 00:00 UTC of 20 July the worm stop the propagation phase. It start now the attack phase where it floods specific address with huge amount of packet and this is what we called DDoS.

The worm stops on 27 July until 1 August where it will make the same phases again.

### **3.4 Collected data on Code Red:**

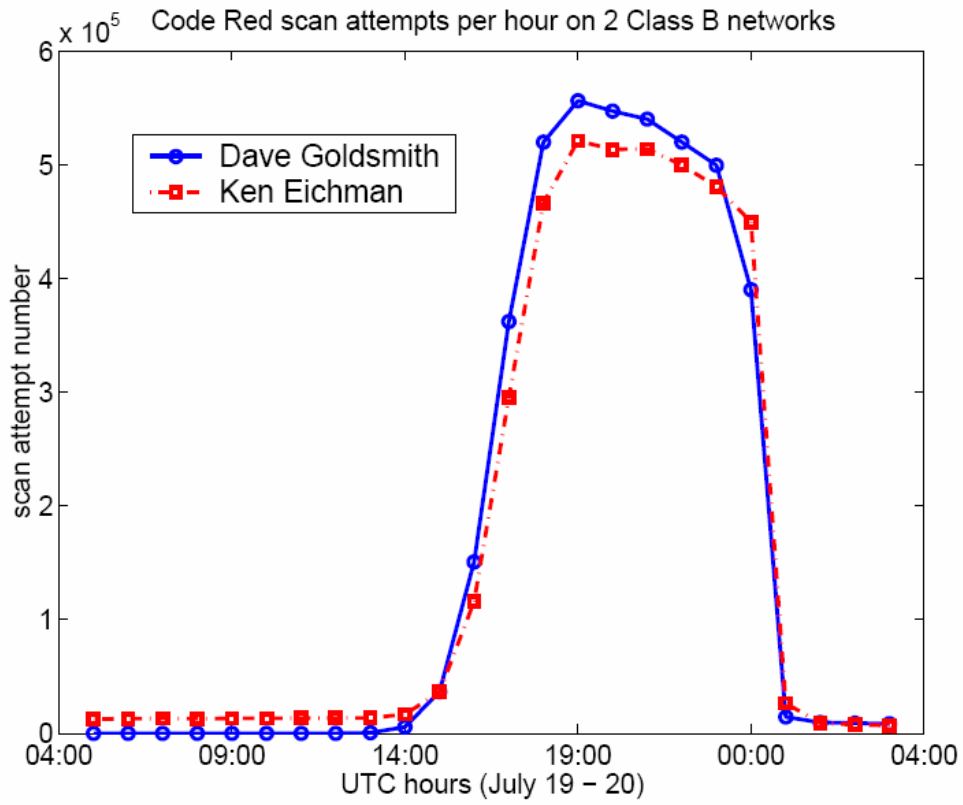
The scientist was afraid of such attack from long time, so many of them were analyzing the traffics on the internet looking for suspicious packets.

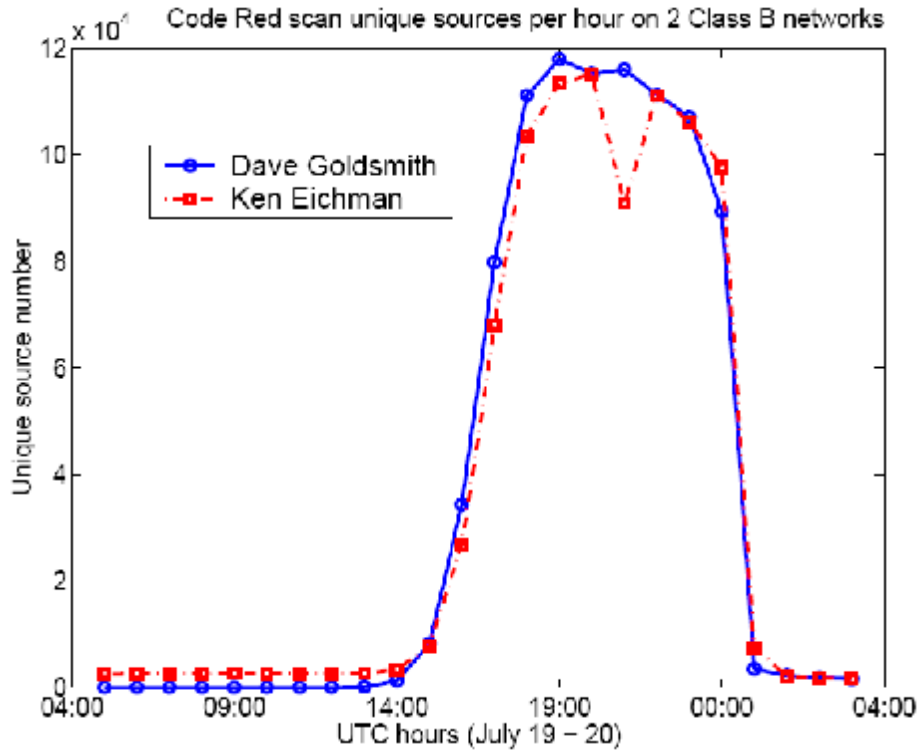
Goldsmith and Eichman registered 2 types of data on 2 different class B networks

- Number of Code Red worm port 80 scans during each hour

- Number of unique sources that generated these scans during each hour.

The following 2 diagrams show the collected data:

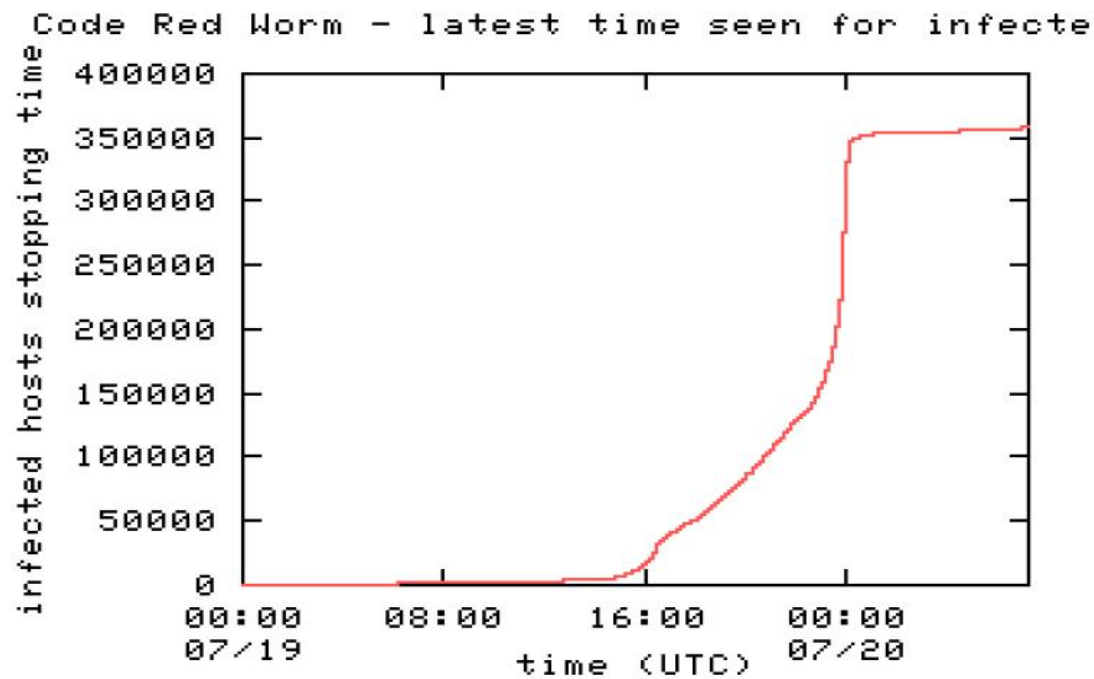
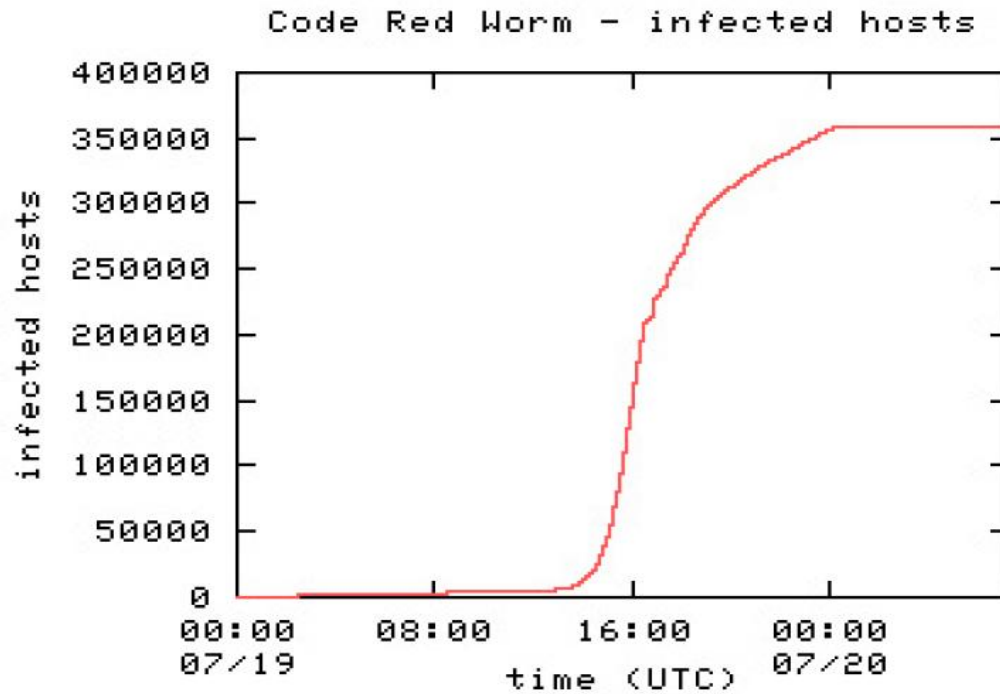




Moore *et al.* recorded the time of the first attempt of each infected host to spread the worm to their networks.

- Number of infected host
- Number of deactivated host

The following 2 diagrams show the collected data:



### 3.5 Modeling the propagation of Code Red:

There is big similarity between Biological Viruses and Computer Viruses and worms, Many Scientist studied the propagation of biological viruses, we can use their results to develop a new model of Computer Worms propagation:

### 3.5.1 Classical simple epidemic model

Each host in one of 2 states: *susceptible* or *infectious*. No removed *state*.

$$dJ(t)/dt = \beta J(t)[N - J(t)]$$

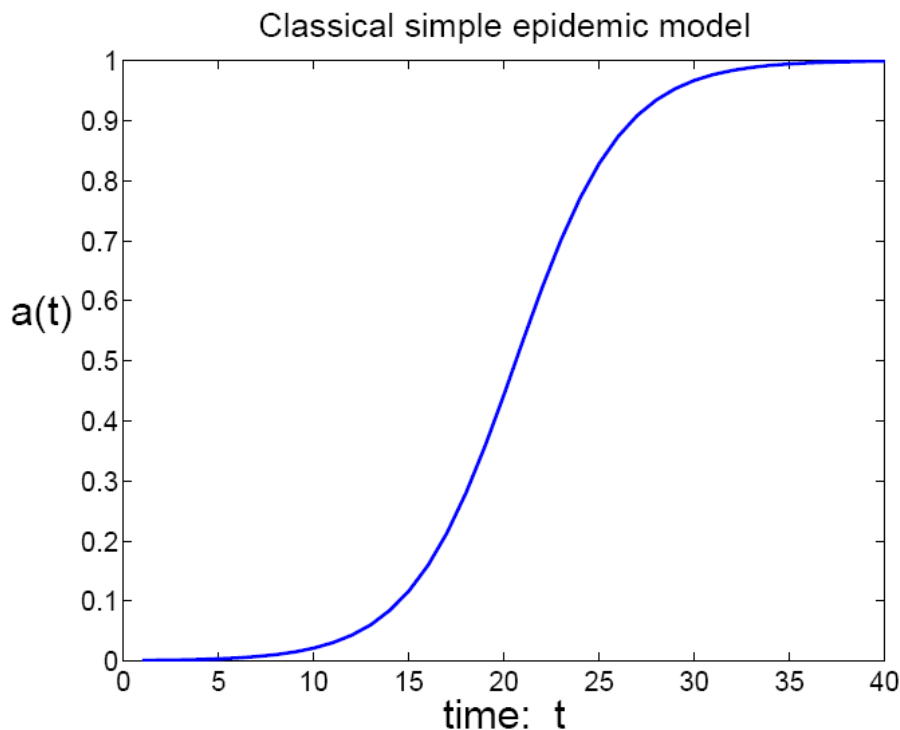
- $J(t)$  is the number of infected hosts at time  $t$ ;
- $N$  is the size of population;
- $\beta$  is the infection rate.

$$\text{Let } a(t) = J(t)/N \Rightarrow da(t)/dt = ka(t)[1 - a(t)]$$

Let  $S(t) = N - J(t)$  the number of susceptible hosts

$$dS(t)/dt = -\beta S(t)[N - S(t)] \text{ Same as } dJ(t)/dt$$

except the minus sign  $\Rightarrow$  Inverse curve.



#### Problems with Classical Simple Model

If we used this model with Code Red worm we should see that at 19:00 UTC almost all online susceptible IIS servers infected. BUT only 60% of the susceptible host has been infected.

### 3.5.2 Classical general epidemic model (Kermack-Mckendrick)

This model considers the removal process of infected hosts (Recover or Die).

We have now 3 states: *susceptible*, *infectious* and *removed*.

$$J(t) = I(t) + R(t).$$

- $I(t)$  the number of infectious hosts at time  $t$ .
- $R(t)$  the number of removed hosts at time  $t$ .
- $J(t)$  the number of infected hosts by time  $t$  (still in infectious state or have been removed)

$$dJ(t)/dt = \beta J(t)[N - J(t)]$$

$$dR(t)/dt = \gamma I(t)$$

$$J(t) = I(t) + R(t) = N - S(t)$$

### Problems with Classical general Model

- In the Internet, countermeasures against worms will remove both susceptible hosts and infectious hosts from circulation. (Search for Vaccine epidemic model)
- This model assumes the infection rate to be constant.

### 3.5.3 Two Factor Worm Model

This model is an improvement of Classical General Epidemic Model, it consider two main points:

- Human countermeasures result in removing both susceptible and infectious computers from circulation (Code Red reschedule on August 1<sup>st</sup> but it did not cause any damage)
- Decreased infection rate  $\beta(t)$ , not a constant rate  $\beta$  — the large-scale worm propagation have caused congestion and troubles to some Internet routers, thus slowed down the Code Red scanning process.

Equations for this model:

$$dS(t)/dt = -\beta(t)S(t)I(t) - dQ(t)/dt$$

$$dR(t)/dt = \gamma I(t)$$

$$dQ(t)/dt = \mu S(t)J(t)$$

$$\beta(t) = \beta_0[1 - I(t)/N]\eta$$

$$N = S(t) + I(t) + R(t) + Q(t)$$

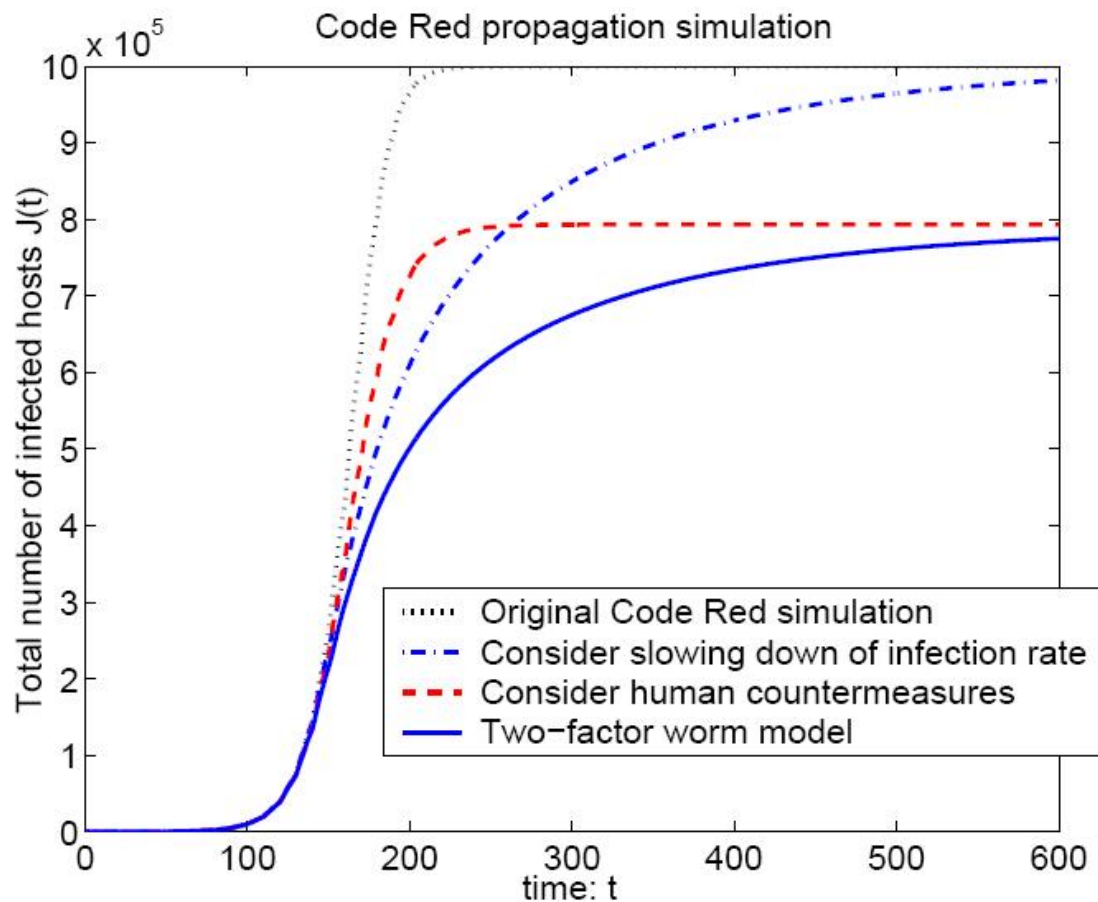
$$I(0) = I_0 \quad N; \quad S(0) = N - I_0; \quad R(0) = Q(0) = 0;$$

Where:

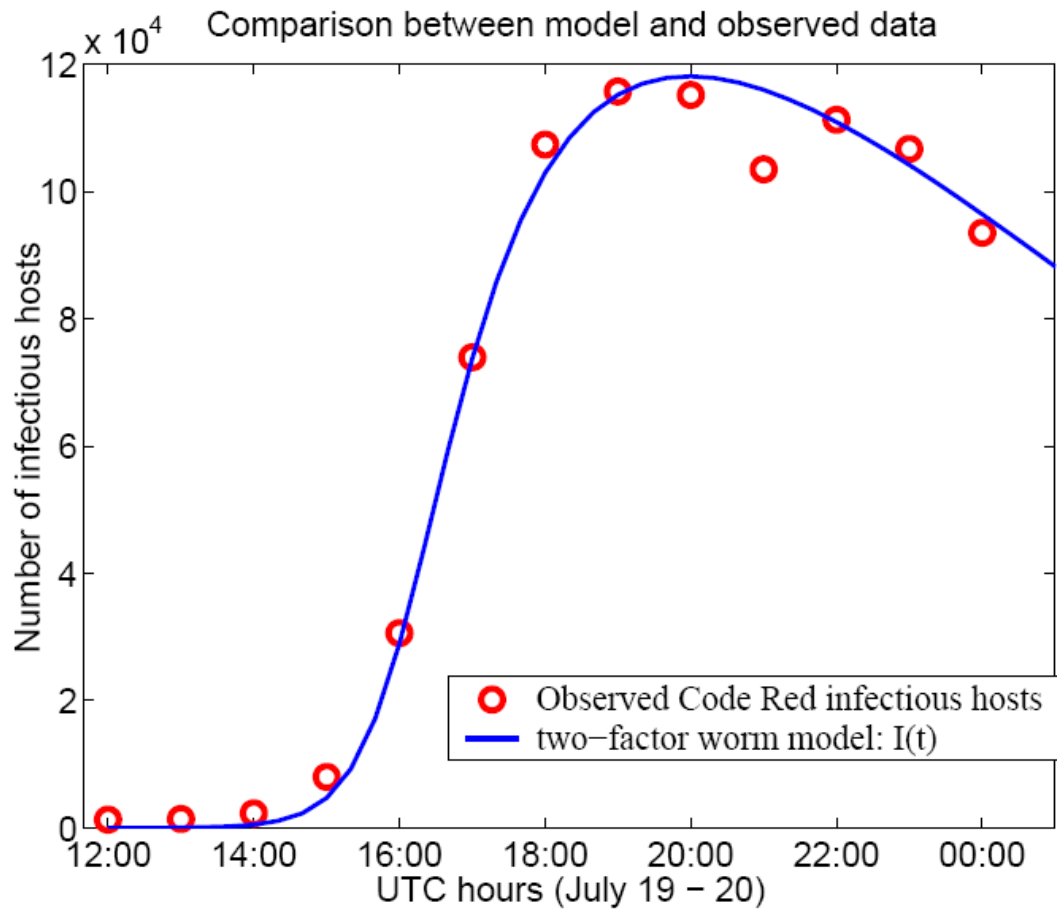
- $S(t)$  Number of susceptible hosts at time  $t$
- $I(t)$  Number of infectious hosts at time  $t$
- $R(t)$  Number of removed hosts from the infectious population at time  $t$

- $Q(t)$  Number of removed hosts from the susceptible population at time  $t$
- $N$  Total number of hosts under consideration,  $N = I(t) + R(t) + Q(t) + S(t)$
- $J(t)$  Number of infected hosts at time  $t$ , i.e.,  $J(t) = I(t) + R(t)$
- $C(t)$  Total number of removed hosts at time  $t$ , i.e.,  $C(t) = R(t) + Q(t)$
- $\beta(t)$  Infection rate at time  $t$
- $D(t)$  Infection delay time in simulation, representing the time for a Code Red worm to find an IIS server

The following diagram represents the different curves that represent each factor in Tow Factor worm model.



The following diagram represents the comparison between observed value and the tow factor model:



## 4. Conclusion and Recommendations

We presented the several types of threat on the internet and focused on worms. We presented some models for representing worm spreading on the internet.

We also demonstrate how worms could make DDoS and the main problem in DDoS is the distribution of the attack entry points and the difficulty to know the origin of the attack with the current infrastructure.

We focused on CodeRed worm since it is the first worm with height loss percentage, about 2.6 billion dollars.

There is no magic solution for worm and DDoS, this fields still good research subject since 10 years, and I it still waiting for a better solution.

## REFERENCES

- [1] Alefiya Hussain, John Heidemann, Christos Papadopoulos, A framework for classifying denial of service attacks, In Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, August 2003.
- [2] Aleksandar Kuzmanovic, Edward W. Knightly, Denial-of-service: Low-rate TCP-targeted denial of service attacks, In Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, August 2003.
- [3] Andrew S. TANENBAUM, 2003, PH PTR, Computer Networks fourth edition.
- [4] Anonymous, 2001, SAMS, Maximum Security Third edition.
- [5] Arno Wagner, Bernhard Plattner, Peer-to-Peer (P2P) systems, are good for DDoS, Swiss Federal Institute of Technology Zurich, Computer Engineering and Networks Laboratory, 2002.
- [6] Arno Wagner, Thomas Dübendorfer, Bernhard Plattner, Roman Hiestand, Network interactions Experiences with worm propagation simulations, in Proceedings of the 2003 ACM workshop on Rapid malware WORM '03, October 2003.
- [7] CAIDA: COOPERATIVE ASSOCIATION FOR INTERNET DATA ANALYSIS Security Data Collection, URL [www.caida.org](http://www.caida.org)
- [8] CERT/CC Statistics, URL [http://www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html).
- [9] Chao Gong, Kamil Sarac, IP Traceback based on Packet Marking and Logging, Department of Computer Science University of Texas at Dallas, USA, 2005.
- [10] Cheng Jin, Haining Wang, Kang G. Shin, Hop-count filtering: an effective defense against spoofed DDoS traffic, Proceedings of the 10th ACM conference on Computer and communications security, October 2003.
- [11] Cliff Changchun Zou, Lixin Gao, Weibo Gong, Don Towsley, Monitoring and early warning for internet worms, In Proceedings of the 10th ACM conference on Computer and communications security, October 2003.
- [12] Cliff Changchun Zou, Weibo Gong, Don Towsley, Code red worm propagation modeling and analysis, in Proceedings of the 9th ACM conference on Computer and communications security November 2002.
- [13] D. Moore and C. Shannon, "Code-Red: a Case Study on the Spread and Victims of an Internet Worm," in Proceedings of the 2002 ACM SIGCOMM Internet Measurement Workshop, Marseille, France, Nov. 2002.

- [14] DEFEATING DDOS ATTACKS, Whitepaper, Cisco Systems, 2004.
- [15] Ed Skoudis, 2002, Counter HACK, Printice Hall.
- [16] Lisa Yeo, 19-Dec-02, Printice Hall PTR, Personal Firewalls for Administrators and Remote Users.
- [17] Marco de Vivo, Eddy Carrasco, Germinal Isern, Gabriela O. de Vivo, A review of port scanning techniques, ACM SIGCOMM Computer Communication Review, Volume 29 Issue 2, April 1999.
- [18] Jelena Mirkovic, D-WARD: Source-End Defense against Distributed Denial-of-Service Attacks, Ph.D. Thesis in University of California Los Angeles, 2003.
- [19] Jelena Mirkovic, Peter Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, ACM SIGCOMM Computer Communication Review, Volume 34 Issue 2, April 2004.
- [20] Prateek Mittal, Defense against Distributed Denial of Service Attacks, A seminar report in Department of Computer Science and Engineering Indian Institute of Technology, April 19, 2005.
- [21] Stéphane Racine , Analysis of Internet Relay Chat Usage by DDoS Zombies, Master Thesis in Swiss Federal Institute of Technology Zurich, Apr 2004.
- [22] Tao Peng, Defending Against Distributed Denial of Service Attacks, Thesis in the University of Melbourne, April 2004.
- [23] Thomas Dübendorfer, Adaptive Distributed Traffic Control Service for DDoS Attack Mitigation, 1st International Workshop on Security in Systems and Networks (SSN 2005) hold in conjunction with IEEE IPDPS 2005 Conference, April 4-8, 2005 in Denver, Colorado.
- [24] Thomas W. Doepfner, Philip N. Klein, Andrew Koyfman, Using router stamping to identify the source of IP packets, In Proceedings of the 7th ACM conference on Computer and communications security, November 2000.
- [25] William Stallings, 2003, Printice Hall PTR, Cryptography and Network security principles & practice 3d edition.
- [26] Wu-chang Feng, The case for TCP/IP puzzles, In Proceedings of the ACM SIGCOMM workshop on Future directions in network architecture FDNA '03, Volume 33 Issue 4, August 2003.
- [27] [www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html](http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html) , 13/7/2006
- [28] [www.us-cert.gov/cas/techalerts/TA04-028A.html](http://www.us-cert.gov/cas/techalerts/TA04-028A.html), 13/7/2006.