Volume 2, No. 1, Jan-Feb 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

A new Methodology to Prevent DDos Attacks using File Watcher and IP Watcher

K.Kuppusamy
Associate Professor, Dept of Comp.Sci and Engineering
Alagappa University,
Karaikudi-India
kkdiksamy@yahoo.com

S.Malathi*
Lecturer in Comp.Sci,
Rabiammal Ahamed Maideen College for Women,
Tiruvarur-India
visitmalathi@gmail.com

Abstract: In the modern computer world, the information is maintained in a file. Some interrupts may occur on the stored data to corrupt the file. This may be termed as **'Attacks'**. There exists lot of attacks that would corrupt our file. One of the common attacks is termed as **DDOS Attack**. To avoid these attacks and to prevent our files, the concept of file watcher, Ip watcher and firewall are used. All our files are saved in the database and the firewall allows all kinds of users to access the files. This kind of permission to access the file has certain limitations such as until the user does not involve in the action of modifying the file. When the file gets modified by an individual, it gets corrupted. To prevent the file from these attacks, the file watcher and Ip watcher are included. File watcher is responsible to monitor the file stored in the home directory and analyze the modifications made in the file. In addition, the IP address that modifies the file can be detected by IP watcher. When the client sends request to modify the file, the file watcher deny the service provided to the user and thus prevent the file from attack. The IP Address of the client who sends attack on the file is blocked by adding its address to the blocked list of the firewall. The clients whose IP Address are in the blocked list can't have permission to access the file further. Thus the file is prevented from the attacks. In this paper, a new method has been proposed to watch the activities taken in the file and to prevent the file from modifications by other users.

Keywords: Blocked list, Deny the service, DDOS Attacks, File Watcher, Firewall, IP Address, Monitor, IP watcher

I. INTRODUCTION

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. It generally consists of the concerted efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.

In a denial-of-service attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting a computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent from accessing email, web sites, online accounts, or other services that rely on the affected computer.

In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. They could then force your computer to send huge amounts of data to a web site or send spam to particular email addresses. The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attack. It occurs when multiple compromised systems flood the bandwidth or resources of a targeted system, usually one or more web servers. These systems are compromised by attackers using a variety of methods.

The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information. When you type a URL for a particular web site into your browser, you are sending a request to that site's computer server to view the page. The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process your request.

An attacker can use spam email messages to launch a similar attack on your email account. By sending many, or large, email messages to the account, an attacker can consume your quota, preventing you from receiving legitimate messages. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers.

One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

An **Internet service provider** (ISP) is considered to be an entity that operates an Internet backbone that is used to carry traffic between two or more other Internet-connected networks. The transport and access to the portions of networks characterize the unique role of an ISP in the context of a distributed-system attack. Packets generated from multiple sources during a distributed denial-of-service attack, for example, are likely to be transported across one or more ISP network backbones en route to the victim site. The access to the portions of an ISP's network may be either components of an attack or the end victim.

In addition to the unique characteristics of the ISP networks, the networked computer systems used by ISPs to deliver services such as DNS, email, and web hosting may

be attractive locations for intruders to install distributed-system tools for several reasons:

A. Active traffic patterns may obscure the use of attack tools.
B. Close proximity to high-capacity network backbones enables attacks to have a high impact.
C. ISP systems themselves may also be high-impact targets for distributed-system attacks.

In a distributed bandwidth denial-of-service attack, the proximity of an ISP to the end victim may have an indirect impact on the ISP and other downstream sites sharing the ISP's network resources. It is possible for portions of an ISP backbone to be overwhelmed, causing degradation and/or denial of service for sites that are not directly targeted in an attack. Coordination among network operators and among sites involved in incidents is essential for diagnosis, tracing, and control of distributed attacks.

The internet service providers (ISP) will be providing their service through the servers. The users getting the service regularly come under the **static mode**. They are always available in the network and use the services through the IP addresses. The **dynamic mode** will be involving devices like Bluetooth for a short period of time. Bluetooth is a wireless protocol for exchanging data over short distances from fixed and mobile devices, creating networks.

Smurf attack is a simple yet effective DDoS attack technique that takes advantage of the ICMP (Internet Control Message Protocol). ICMP is normally used on the internet for error handling and for passing control messages. One of its capabilities is to contact a host to see if it is "up" by sending an "echo request" packet.

The common "**ping**" program uses this functionality. *Smurf* is installed on a computer using a stolen account, and then continuously "pings" one or more networks of computers using a forged source address. This causes all the computers to respond to a different computer than actually sent the packet.

The forged source address, which is the actual target of the attack, is then overwhelmed by response traffic. The computer networks that respond to the forged ("spoofed") packet serve as unwitting accomplices to the attack.

In order for *smurf* to work, it must find attack platforms that have IP broadcast functionality enabled on their routers. This functionality allows *smurf* to send a single forged ping packet and have it broadcast to an entire network of computers. To prevent your system from being used as a *smurf* attack platform, disable IP-directed broadcast functionality on all routers. Generally speaking, this functionality will not be missed.

In order for the attacker to successfully take advantage of you as an attack platform, your routers must allow packets to exit the network with source addresses that do not originate from your internal network. It is possible to configure your routers to filter out packets which do not originate from your internal network. This is known as network egress filtering.

ISP's should employ network ingress filtering, which drops packets which do not originate from a known range of IP addresses. If you are the target of an attack, ask your ISP to also filter out and drop echo reply packets. If you do not want to completely disable echo reply, then you can selectively drop echo reply packets that are addressed to your high-profile, public web servers.

Trinoo is a complex DDoS tool that uses "master" programs to automate the control of any number of "agent" programs which launch the actual attack. The attacker connects to the computer hosting the master program, starts the master, and the master takes care of starting all of the agent programs based on a list of IP addresses. The agent programs then attack one or more targets by flooding the network with UDP packets. Prior to the attack, the perpetrator will have compromised the computer hosting the master programs and all the computers hosting the agent program in order to install the software.

Trinoo uses UDP protocol for all communications between the master program and the agents. Intrusion Detection Software can look for flows that use UDP protocol. T*rinoo* master programs listen on port 27655. The attacker will connect via TCP, typically via Telnet, to the computer hosting the master program to launch it. Intrusion Detection Software can look for flows that use TCP (type 6) to connect to port 27655.

II. RELATED WORK

In paper[1], they propose an inter-domain packet filter (IDPF) architecture that can mitigate the level of IP spoofing on the Internet. IDPFs are constructed from the information implicit in BGP route updates and are deployed in network border routers and also they proposed and studied an inter-domain packet filter (IDPF) architecture as an effective countermeasure to the IP spoofing-based DDoS attacks.

Distributed Denial of Service (DDoS) attacks pose an increasingly grave threat to the Internet, as evidenced by recent DDoS attacks mounted on both popular Internet sites [3] and the Internet infrastructure [2]. Alarmingly, DDoS attacks are observed on a daily basis on most of the large backbone networks [4].

One of the factors that complicates the mechanisms for policing such attacks is IP spoofing, the act of forging the source addresses in IP packets. By masquerading as a different host, an attacker can hide its actual identity and location, rendering source-based packet filtering less effective. It has been shown that a large part of the Internet is vulnerable to IP spoofing [5], [6].

Recently, there is anecdotal evidence of attackers to stage attacks utilizing bot-nets1 [7]. In this case, since the attacks are carried out through intermediaries, i.e., the compromised .bots, it is tempting to believe that the use of IP spoofing is less of a factor than previously. However, recent studies present evidence to the contrary and show that IP spoofing is still a commonly observed phenomenon [8], [9].

Denial of service (DoS) is a pressing problem on the Internet as evidenced by recent attacks on commercial servers and ISPs and their consequent disruption of services [10]. DoS attacks [11], [12], [13], [14], [15] consume resources associated with various network elements—e.g.,Theyb servers, routers, firewalls, and end hosts—which impedes the efficient functioning and provisioning of services in accordance with their intended purpose.

A number of recent works have studied the problem of tracing the physical source of a DoS attack [16], [17], [18], [19], [20]. In deterministic packet marking [21], the source of a traffic flow is recovered by employing tracing

information inscribed in the packet. Packet marking can be viewed as a form of "stateless logging" which emulates the capability of path recovery by router based information logging [19], without incurring the latter's status and associated space overhead. A related method is messaging based path recovery which uses control messages emitted from routers conveying path information to destination nodes. Thus (router) statelessness is achieved, however, at the cost of message overhead.

Several types of DoS attacks have been identified [10], [12], [23], [14] with the most basic DoS attack demanding more resources than the target system or network can supply. Resources may be network bandwidth, file system space, processes, or network connections [23]. While host-based DoS attacks are more easily traced and managed, network-based DoS attacks which exploit the weaknesses of the TCP/IP protocol suite represent a more subtle and challenging threat [23], [16]. Network-based DoS attacks, by default, employ spoofing to forge the source address of DoS packets to hide the identity of the physical source [15].

A number of recent works have studied source identification (also called IP traceback in [16]) which spans a range of techniques with their individual pros and cons

The principal contribution of [16] lies in the investigation of coding issues aimed at further reducing the (constant) marking bits needed in the IP header via fragmentation. The IP option field is another possible candidate for implementing marking field coding.

Firewalls offer a protection for private networks against both internal and external attacks. However, configuring firewalls to ensure the protections is a difficult task. The main reason is the lack of methodology to analyze the security of firewall configurations. IP spoofing attack is an attack in which an attacker can impersonate another person towards a victim. In the paper [22], they propose a new methodology for verifying the vulnerability of firewall configurations to IP spoofing attack and for synthesizing IP spoofing-free configurations. The methodology is based on graph theory which provides a simple and intuitive approach to the vulnerability analysis of the attack.

In this paper, we implement the much better technology by analyzing the above mentioned papers.

III. METHODOLOGY

A. Proposed Method

The aim of the proposed method is to watch the activities taken in the file and prevent the file from modifications by the other users.

An intruder can change the IP address without the knowledge of web server at any time means **IP Spoofing**. We can provide any kind of address and can change it often. Usually the machine contains 2 kinds of addresses are IP Address, MAC Address.

In case of network, each machines address is stored in the database. If the server receives any request from the client, first it finds the IP Address and MAC Address of the client's machine and compares it with the database.

If the comparison returns true, it sends the response to the client's request. If it is found to be incorrect, it treats the client machine as Hacker and Block the IP Address and also it does not send any kind of response to the client. Thus it provides security to the machine and keeps the data secure from any unwanted access. Figure 1 illustrates this process.

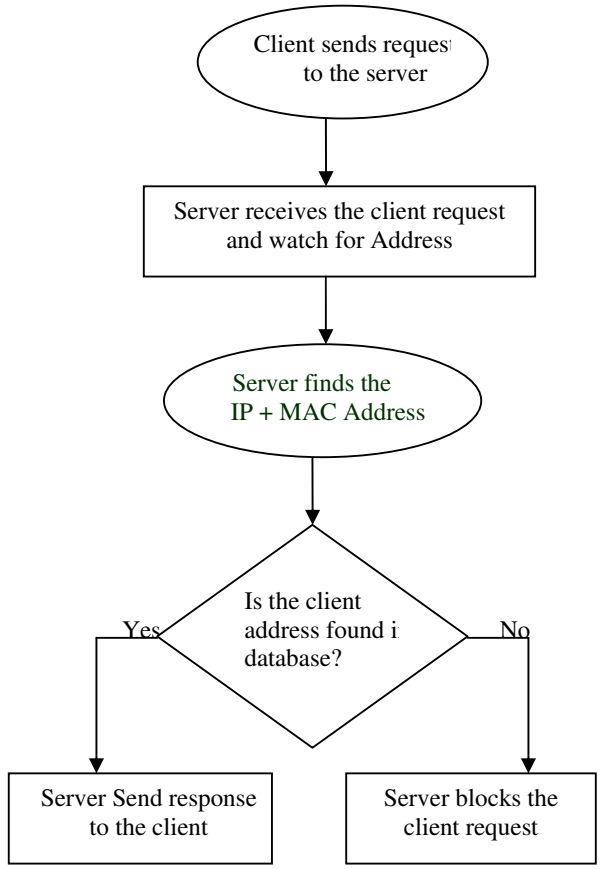

Figure-1: Response for the client request

The new methodology is implemented by using the following steps to handle the DDoS problem.

Step 1: A **Web Server** is software that answers requests for documents from web clients. Over the internet, all web servers use a language, or protocol to communicate with web clients called the Hyper Text Transfer Protocol (HTTP). All type of data can be exchanged using this protocol including HTML, Graphics sound and Video HTTP is a stateless protocol, which means there is no continuous connection between the client and server. Any server machine makes it services available to the internet using numbered ports one for each service that is available on the server. A web server would typically be available on Port80. Clients connected to a service at a specified IP Address and on a specific port web server monitoring the client information. For data being accessed at a time, to monitor the IP Address, Host, Date, Time, and File Name.

Web server maintains personal filter. It allows only for the authorized person for login the server to access the files. A web server is a computer program that delivers content such as web pages using HTTP GET requests.

The primary functions of the web server are to deliver the web page to the client according to their respective requests. A webpage may contain html documents and other

documents that include the images styles sheets and java scripts.

Step 2: Web client will make a request to web server and it will respond with asking for specific filename. It will be access to only for authorized person. It will not be access to an unauthorized person. It will provide you restricted data to login the web server after ascertaining the username and password to check and then files will be available from the restricted data.

Here a temporary web server is created by using the predefined functions that are to be compulsorily present while creating a web server and it is allowed to be used by the clients.

The clients those who are accessing the web server may be authorized users or unauthorized persons. The users who access to the webpage for reasonable works are called authorized users. They will use the web page in a correct way by making a HTTP request following their needed file name. While doing like this they will get the requested file as the output from the web server. In the same way an authorized client can also use the web server.

On the other side the work of the unauthorized users or attackers is that they will attack the victim web server to make the server down. They may do this job by a number of HTTP GET requests and pulling large image files from the server in overwhelming numbers .In another instance, attackers run a massive number of queries through the victim's search engine or database query to bring the server down. The created web server has to be protected from the attackers and its applications are accessed by various users.

Webserver will be maintaining the databases for request and response for client information for ip address, host, time, date, file name. This data will be stored in the databases web server called **log entry** will be monitoring the spiced date for how many number of clients will be access at the specified date.

These entries serve as the log for all the clients. Once a client had a login to the browser the details of the client is maintained in a database.

IP address, time of access, number of files accessed, name of file accessed are stored in the database. Whenever a client access to the website the database is updated with the new client details.

This database serves as the main evidence to differentiate the users logged on to the web server when there is normal rate of entry for a particular user in this database they are considered as the normal users accessing the server for proper needs. At each time a user enter into the server their details are maintained separately for each and every access of that particular user.

Step 3: IP watcher is a network security and administrative tool. This tool can control the unencrypted login on network. It is an extremely valuable tool for investigating suspicious activity. This tool is used for obtaining the evidence of misusers and even stopping malicious users before they do any damage in the network.

IP watcher is used to separate the misusers from the list of users those who are logging into the web server for accessing the files. The log entry module paves the way for this activity since it has the database of the users. From the second module's details IP watcher will perform a work of watching the all the client's IP addresses and it will maintain a separate list for the users who were accessing the site obviously within a threshold limit. These details are in a database namely blocked IP.

Security measures can be done as follows, User name is validated with server database. Password is validated with server database. While creating new user the password is confined Password length is limited to maximum of 8 characters, mimimum of 2 characters and one special character should be there. While changing the password the password has to confine.

Step 4: DDoS checker performs the function of checking the users those who were accessing the server for using its applications. Each and every user's ip address is checked with the blocked ip database and then only they will be provided with their required files.

It is used to check the separated DDoS attackers from the legitimate users. When a very large number of users simultaneously access to a website it produces a surge in traffic and it will make the website virtually unreachable. These users are also identified as the attackers and their ip addresses are added to the blocked IP list .In this session the attackers are listed by using the details like the number times they access to the server and the kind of files requested by them. Only after the checking process, they can get the file or instructions they requested from the web server.

Step 5: This is the final step that produces the output to the attackers. This is performed by using the database and for that particular user in the blocked ip list. When the client having the IP address in blocked list access to the website there will not be any response to that clients. Their request for accessing the files will not be processed and their right to access the website is denied, since that particular user is in the **DDoS list.**

Thus the client who accesses to the web site is checked by using their IP address and the types of files they need to get from the server. Then they are produced with the corresponding output based on the user's application.

B. Algorithm

```
Start the process
Analyse the Files to be kept secure
Count the number of file in the list
For i=1 to count
{
   Store the files in the Home Directory
   Assign each file with a Log Id
   Store the file in the database with the Id
}
While (time period to keep the file secure)
{
   Watch the file
    Identify the file log Id
    New-id = file.log id
    For i=1 to count
{
   If (File(i).old-Id == New-id) then
   The file is secure.  Leave it from any modification
   Else
```

Restore the original file from the backup directory.
}
}
Stop the process

C. Algorithm Explanation

The explanation for the proposed algorithm is as follows:

First step of the algorithm is to get the list of file names that must be kept secure from the attacks. Then count the number of files in the list. Assign unique ID for each file in the Home Directory and then kept the files in the database.

Each time when the user accesses to the file, the file watcher identifies the Log id for that file and then compares it with original Log Id which is kept in the database. If both Id are found to be same, then the file watcher identifies that the file is the original file and leave the file from further replacement. Otherwise, the file is replaced by the original file which is stored in the Backup Directory. Thus the file watcher watches the file and prevents the file from attacks.

Thus the proposed algorithm is sufficient to satisfy our requirements of preventing the file from attacks.

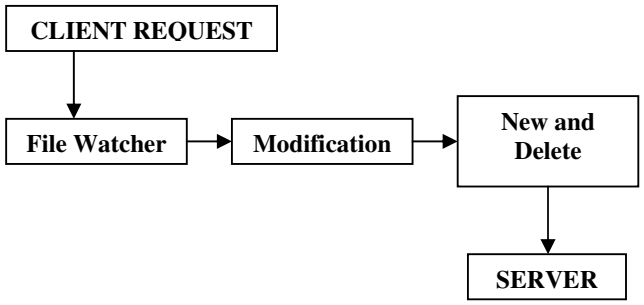

Figure-2: Process of File Watcher

IV. EXPERIMENTAL RESULTS

The implementation of the file watcher technique is essential to make the file secure from attacks. There may be more number of files in the database. When the user enters into the site and wants to access the file from the database, the firewall provides permission to the user to access the file. The file watcher continuously watches the file and identifies the user who modifies the file. When the client sends request to hack the file or to modify the file, the file watcher identifies them as '**Hacker'** and restrict them to modify the file.

The file watcher then stores the IP Address of the hacker in the Denial List of the firewall that address detected by IP watcher and then replaces the file from the home directory. When another client enters into the site to access the file, the firewall locates the IP Address of that client and matches it with the IP Addresses in the blocked list. If the IP Address found in the Blocked list, it denies the access of that client.

Thus the file watcher, Ip watcher and the firewall help us to keep our file secure from the attacks by blocking the hackers.

V. CONCLUSION

In this paper we have discussed the strategies made to tackle the continuous threats disturbing the internet services.

It has the command for user friendly environment the ability to store user profiles, properly maintaining the database to retrieve the files and profiles and sending them to the server component aided by computer speed high memory capacity and accuracy.

This have the advantage of differentiating the clients from the attackers those who tries to affect the server function by posting requests in a large amount for unwanted reasons. This can be used for creating defenses for attacks require monitoring dynamic network activities.

The basic idea behind the proposed system is to isolate and protect the web server from huge volumes of DDoS request when an attack occurs. In particular, we propose a DDoS defense system for protecting the web services. It is of paramount importance because the web is the core technology under-lying E-commerce and the primary target for DDoS attacks. When a DDoS attack occurs, the proposed defense system ensures that, in a web transaction, the web server information are managed without corruption.

This newly designed system that effectively sustains the availability of web services even during severe DDoS attacks. Our system is practical and easily deployable because it is transparent to both web servers and clients and is fully compatible with all existing network protocols. Since the web is the core technology underlying e-commerce and a primary target for recent DDoS attacks, this work offers a practical solution to a very important security problem.

VI. REFERENCES

[1] "Constructing Inter-Domain Packet Filters to Control IP Spoofing Based on BGP Updates" by Zhenhai Duan, Xin Yuan, Jaideep Chandrashekar.
[2] Massive DDoS attack hit DNS root servers. http://www. internetnews.com/ent-news/article.php/1486981, October 2002.
[3] Yahoo attributes a lengthy service failure to an attack. http://www.nytimes.com/library/tech/00/02/biztech/ articles/08yahoo.html%, February 2000.
[4] Craig Labovitz, Danny McPherson, and Farnam Jahanian. Infrastructure attack detection and mitigation. SIGCOMM 2005, August 2005. Tutorial.
[5] R. Beverly. Spoofer project. http://momo.lcs.mit.edu/ spoofer.
[6] R. Beverly and S. Bauer. The Spoofer Project: Inferring the extent of Internet source address _ltering on the internet. In Proceedings of Usenix Steps to Reducing Unwanted Traf_c on the Internet Workshop SRUTI'05, Cambridge, MA, July 2005.
[7] Srikanth Kandula, Dina Katabi, Matthais Jacob, and Arthur Berger. Botz-4-Sale: Surviving Organized DDoS Attacks that Mimic Flash Crowds. In Second Symposium on Networked Systems Design and Implementation (NSDI'05)., 2005.
[8] D. Moore, G. Voelker, and S. Savage. Inferring internet Denial-of-Service activity. In Proceedings of 10th Usenix Security Symposium,August 2001.

[9] R. Pang, V. Yegneswaran, P. Barford, V. Paxson, and L. Peterson. Characteristics of internet background radiation. In Proceedings of ACM Internet Measurement Conference, October 2004.
[10] Lee Garber, "Denial-of-service attacks rip the Internet," Computer, pp.12–17, Apr. 2000.
[11] John Elliott, "Distributed denial of service attack and the zombie ant effect," IT Professional, pp. 55–57, March/April 2000.
[12] Jari Hautio and Tom Weckstrom, "Denial of service attacks," Mar. 1999, http://www.hut.fi/u/tweckstr/hakkeri/DoS paper.html.
[13] John D. Howard, An Analysis of Security Incidents on the Internet, Ph.D. thesis, Carnegie Mellon Univerisity, Aug. 1998.
[14] Computer Emergency Response Team, "Denial of service," Feb. 1999, Tech Tips, http://www.cert.org/tech tips/denial of service.html.
[15] Computer Emergency Response Team (CERT), "CERT Advisory CA-2000-01 Denial-of-service developments," Jan. 2000, http://www.cert.org/advisories/CA-2000-01.html.
[16] Stefan Savage, David Wetherall, Anna Karlin, and Tom Anderson, "Practical network support for IP traceback," in Proc. of ACM SIGCOMM, Aug. 2000, pp. 295–306.
[17] Steven M. Bellovin, "ICMP traceback messages," Mar. 2000, Internet Draft: draft-bellovin-itrace-00.txt (expires September 2000).
[18] Cisco Systems, "Characterizing and tracing packet floods using Cisco routers," Aug 1999.
[19] Dawn Song and Adrian Perrig, "Advanced and authenticated marking schemes for IP traceback," Tech. Rep. UCB/CSD-00-1107, Computer Science Department, University of California, Berkeley, 2000.
[20] Robert Stone, "Centertrack: An IP overlay network for tracking DoS floods," in Proc. of 9th USENIX Security Symposium, Aug. 2000.
[21] H. Burch and B. Cheswick, "Tracing anonymous packets to their approximate source," Dec. 1999, unpublished manuscript.
[22] "A graph-based Methodology for Analyzing IP spoofing Attack", Voravud Santiraveewan and Yongyuth Permpoontanalarp, Logic and Security Laboratory, Thailand.
[23] NightAxis and Rain Forest Puppy, "Purgatory 101: Learning to cope with the SYNs of the Internet," 2000, some practical approaches to introducing accountability and responsibility on the publicinternet,http://packetstorm.securify.com/papers/contest/RFP.doc.