Volume : 2 | Issue : 7 | July 2013 • ISSN No 2277 - 8160



Research Paper | Computer Science

The Internet and freedom of expression and its new regulatory schemes implemented by private parties

Mr. Sumit Patel

Assistant Professor, Shree Swaminarayan Institute of Technology, Gandhinagar, Gujarat, India-382428

ABSTRACT

Internet challenges the right to freedom of expression. On one side hand, Internet empowers freedom of expression. On the other hand, the free flow of information has raised the call for content regulation, not least to restrict minors' access to potentially harmful information. This schism has led to legal attempts to regulate content and to new self regulatory schemes implemented by private parties. The attempts to regulate content raise the question of how to define Internet in terms of "public sphere" and accordingly protect online rights of expression. The paper will argue that Internet has strong public sphere elements, and should receive the same level of protection, which has been given to rights of expression in the physical world. Regarding the tendency towards self regulation, the paper will point to the problem of having private parties manage a public sphere, hence regulate according to commercial codes of consumer demand rather than the principles inherent in the rights of expressions, such as the right of every minority to voice her opinion. The paper will conclude that the time has come for states to take on their responsibility and strengthen the protection of freedom of expression on Internet.

KEYWORDS : System, lifeworld, Internet security, internet regulation, CDA(Communication Decency Act), COPA (Child Online Protection Act), CHIPA(Children's Internet Protection Act), B46, PICS(Platform for Internet Content Selection).

INTRODUCTION

Freedom of expression on the internet first in the United States the freedom of expression is guaranteed in the first Article of Amendment to the American Constitution. It states, "Congress shall make no law. It does not establish the freedom of expression, but rather, in recognizing its existence, guarantees it. In his 1998 report to the U.N. Commission on Human Rights, the Special Reporter on the promotion and protection of the right to freedom of opinion and expression outlined the case against government regulation of Internet access and content as follow: "The new technologies and, in particular, the Internet provide the public and individuals with access to information and sources and enable all to participate actively in this communication process.

In December 2000, the United States Congress passed the CHIPA, which requires schools and libraries for protection to shield minors from adult content.

PICS Rules implementation of server/proxy based filtering, beyond the control of end-user.

Individual library patrons will now challenge the federal law that mandates the list of filtering software in schools and libraries receiving federal grants for computers or Internet access.

In January 2001, a Danish public library announced that it had made filtering mandatory on its public computers, in order to block access to pornography and harmful material for both adults and minors.

Internet challenges the right to freedom of expression safeguarded in the international human rights treaties. On the one hand, Internet empowers freedom of expression by providing individuals with new means of imparting and seeking information. On the other hand, the free flow of information has raised the call for content regulation, not least to restrict minors' access to potentially harmful information.

In the US the call for state intervention has so far led to the US CDA in 1996, the COPA in 1998, and the CHIPA in 2000.

AIM OF PAPER

As a legal basis, the dissertation will use Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and the elated case law of the European Court. The level of protection provided for be the right to freedom of expression will be discussed by examining the scope of application of Article 10. The legal assessment will include some current policy tendencies in the field of freedom of expression and Internet.

In order to define the legal and political space so far defined for online content regulation, some recent cases will be examined. The cases will primarily deal with two types of content regulation, namely state legislative measures and self-regulatory schemes.

The final part of the dissertation will discuss the level of protection that should be provided for online expressions, including the issue of positive state obligations in order to protect freedom of expression in a communicative sphere managed by private parties.

WHAT IS THE CASE FOR SOME FORM OF REGULATION?

Internet is open for everybody

First internet establishes for US military. Then it was broadened to the American academic community; next it grew to academic communities in other industrialized countries; now the Internet has users in every country in every age group. Today the Internet can be accessed by a young child from the privacy of her bedroom at any time of the day or night.

Internet is like other electronic network media

In 1996, the European Commission noted: "A unique characteristic of the Internet is that it functions simultaneously as a medium for publishing and for communication. Unlike in the ease of traditional media, the Internet supports a variety of communication modes: one-to-one, one-to-many, and many-to-many. An Internet user may "speak" or "listen" interchangeably. The Internet therefore is radically different from traditional broadcasting. Internet is like radio, television, and publication but effective electronic network for communication.

There is harmful and offensive content on the Internet also criminal activities on internet.

The major problem here is child pornography and sexual solicitation of children. On internet child pornography also display it is harmful. In most cases, the production of this material has involved child abuse; in many cases, the users of such material are interested in. We cannot simply accept this as the price for freedom of expression. In most countries, mere possession of child pornography is a criminal offence whether this occurs off-line or on-line.

There is a massive amount of pornography of all kinds on the Internet. Many children on-line have come act While almost all of this is legal and a free society should permit access to such material, many Internet users – especially parents, teachers and those with responsibility for children – will want to place some limitation on access to such material. So web sites that upset or uncomfortable them. Some people use it for a wide range of disreputable activity, much of which is illegal in most jurisdictions. Such activity includes copyright theft, credit card fraud, financial scams, money laundering, hacking, industrial espionage, cyber terrorism, actual terrorism, bomb making instructions, prostitution, certain forms of gambling, drug use, drug smuggling, suicide assistance, defamatory allegations, cyber stalking.

Users want some form of control or regulation

So people want control or regulations which are make by government and private parties.

VARIOUS FORMS OF REGULATION
The constitutional approach of regulation

The restrictions, which are admissible according to paragraph, fall in to three categories:
- Protection of the public interest
- Protection of other individual rights
- Necessity of maintaining the authority and impartiality of the judiciary.

Whereas the first and third point concerns restrictions referring or the interest of the system, the second point concerns restrictions referring to lifeworld, which is the freedoms of other individuals.

A key concept entailed in paragraph is that of "*duties responsibilities*". Duties and responsibilities play a particularly important part in three circumstances. Firstly in case regarding freedom of the press, secondly in cases where that person possesses a special status, and thirdly in cases where the protection of morals in involved.

The Court has often stressed that it is now on the press to impart information and ideas on political issues as well as other areas of public interest. "Not only does the press have the task of imparting such information and ideas: the public also has a right to receive them". Accordingly, restrictions on freedom of expression here the press in involved are interpreted narrowly by the Court. Also, several cases have been raised concerning the issue of restrictions on persons with special status, such as soldiers, teachers, civil servants. Case law shows that the Court does not easily accept restrictions on freedom of expression due to special "duties and responsibilities' on these groups. Finally, duties and responsibilities play and important part in cases where the "protection of morals" is invoked to justify a restriction on freedom of expression. Thus the system of state authorities can – to a relatively strong degree – invoke the protection of morals as a legitimate ground for restricting individuals' freedom of expression.

When assessing a restriction on freedom of expression. the Court applies a three-part test (1) The restriction must be prescribed by law and meet the corresponding criteria of precision and accessibility, (2) it must have a legitimate aim as provided (3) it must he "necessary in a democratic society". The necessity test is the ultimate and decisive criterion for the Court. When assessing the proportionality of the restriction in question, the Court examines whether the formalities, conditions, restrictions of penalties imposed on the exercise of freedom of expressions, restrictions or penalties imposed on the exercise of freedom of expression are proportionate to the legitimate aim pursued, that is the restriction should not be overbroad nor be permitted if a less restrictive alternative would serve the same goal.

State control approach of regulation
This approach is adopted by governments which believe that they have a right - and even a responsibility - to intervene directly and place technical controls on the content that can be accessed by their citizens. A case is Saudi Arabia where all of the country's Internet service providers have to go through a central node where the Saudi authorities block access to sites hosting pornography. In China, all Internet cafes are required to keep records of sites visited, with the aim of preventing access to sites featuring pornography, gambling and those that "harm national unification, sovereignty and territorial integrity". Congress of the Chinese Communist Party in November 2002, the authorities even blocked all access to the Google search engine for a time. Other countries where the state is endeavoring to limit access to the Internet by its citizens include Algeria, Yemen, Bahrain, United Arab Emirates, North Korea, Vietnam, Iran, the Maldives and Singapore.

Self-regulation approach of regulation
Internet content and service providers act in accordance with principles of social responsibility. Internet providers hosting content have an obligation to remove illegal content when they are informed that such content exists.

A service provider may include in its contracts with users and content providers terms that allow it to comply with its legal obligations and protect it from liability. It is in the best interest of industry to take on such responsibility since it enhances consumer confidence and is ultimately good for business. To be effective, codes of conduct must be the product of and be enforced by self-regulatory agencies. Such agencies must be broadly representative and accessible to all relevant parties. Effective self-regulation requires active consumer and citizen consultation by such agencies. Without user involvement, a self-regulatory mechanism will not accurately reflect user needs, will not be effective in delivering the standards it promotes, and will fail to create confidence. In any discussion of Internet regulation, understandably the issue arises of the liability of ISPs. To what extent should ISPs be liable for hosting child pornography or racist content or material which is libelous or material which is in breach of copyright?

One view is that ISPs should have no liability. According to this view, ISPs are simply common carriers like the postal or telecommunications service and therefore should have no liability for the material which they carry. This view is nonsense. A letter or a telephone call is a private communication, whereas a web site or a newsgroup is accessible to a couple of billion Internet users world-wide.

Another view is that ISPs should have strict liability. According to this view, ISPs are publishers like newspapers or magazines or broadcasters and should be held fully responsible for any material which they host or, in effect, publish. This is equal nonsense. The sheer number of web sites and blogs and the frequency with which new material is being added to them mean there is no way those ISPs can know the detailed content of all the material and services which they are hosting or institute processes for checking content before it becomes accessible. For instance, You Tube has more than 20 hours of video uploaded every minute worldwide.

ISPs liable in advance for all the material they host, once an ISP has been given notice of material of doubtful legality, and then there is a liability on that ISP. If the ISP removes the offending material within a reasonable period of time of the notice being received, then generally one would not expect a court to convict, even if the material in question was subsequently found to be illegal.

Rating and filtering techniques
Individuals' right to express opinions and impart information is addressed most thoroughly in CDA and COPA. However, whereas COPA is directed at commercial parties, CDA imposes restrictions on all Internet communications, whether these originate from individuals, non-profit organizations or commercial parties.

The communication at issue, whether denominated "indecent" or "patently offensive" is entitled to constitutional protection and the CDA as a government-imposed content-based restriction on speech must only be upheld it is justified by a compelling government interest and if it is narrowly tailored to effectuate that interest. For instance, each of the two parts of the CDA uses a different linguistic form. The first uses the word "indecent", while the second speaks of material that "in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs". The linguistic vagueness combined with the severity of CDA's criminal penalties "may well cause speakers to remain silent rather than communicate even arguably unlawful words, ideas and images". The Court found that the uncertainty of the terms used undermines the likelihood that the CDA has been narrowly tailored to the goal of protecting minors from potentially harmful material. Thus the scope of the Act being overly broad was a main defect found by the Court. The Court confirmed that the government has a compelling interest in protecting children, but argued that although the protection of children is an important goal, it should not interfere with the legitimate rights of adults to speak or listen to matters not fit for children. As an example, the Court mentions chat rooms. If, for instance, an adult knows that one or more members of a 100 person chat group is a minor, and it therefore would be a crime to send the group an indecent message, this would surely burden communication among adults When assessing CDA's likely effect on the free availability of online material, the Courts found that in many cases it would be either technologically impossible or economically prohibitive to comply with the CDA without impeding the posting of online material, which adults have a constitutional right to access .

Online speakers "talking" through chat rooms or newsgroups have no practical means of controlling who receives the information, neither can content providers determine the identity and age of every user accessing their material. Implementation of age verification systems would place an inappropriate burden not least on individuals and non-profit organizations. Concerning the affirmative defenses in CDA, the Court concluded that such defenses would not be feasible for most noncommercial web publishers, and that even with respect to commercial publishers, the technology had yet to be proven effective in shielding minors from harmful material.

In COPA the scope of communications was narrowed to "web communications made for commercial purposes". Commercial purposes were defined as those individuals or entities that are "engaged in the business of making such communications". In narrowing the scope of communications, COPA sought to encompass the Supreme Court's criticism of the CDA's wide scope. However, when assessing COPA, the Court again stressed that web publishers cannot prevent users from certain geographical districts. The District Court on COPA also discussed the costs and burdens COPA imposes on web publishers and on the adults who seek access to sites covered by COPA. The Court found that the only affirmative defenses available were the implementation of credit card or age verification systems, and that either system would impose significant residual or indirect burdens upon web publishers. Both systems would require an individual seeking to access material, otherwise permissible to adults, to reveal personal information. Because of the likelihood that many adults would choose not to reveal this personal information, websites complying with COPA might experience a loss of traffic, thus be discriminated compared to other commercial sites simply because they contained material, which might be harmful to minors.

Furthermore, the difficulty in shielding minors from potentially harmful content might lead web publishers to censor more information than necessary. Therefore, both CDA and COPA would impose a disproportionate burden on web publishers, and might have a negative effect on the free availability of constitutionally protected material. The Court concluded that the government lacks an interest in enforcing an unlawful law, and that "losing First Amendment freedoms, even if only for a moment, constitutes irreparable harm". In both the CDA and COPA, the notion of "indecency" is defined in terms of "community standards" Since Internet communication is global this would imply that any communication available to a worldwide audience would be judged by the standards of the community most likely to be offended by the message.

Accordingly a parent who sent his 17 year old college freshman information on birth control via e-mail could - according to CDA - be imprisoned even though neither he, his child, nor anyone in their home community, found the material "indecent" or "patently offensive," if the college town's community thought otherwise. The regulated communication might also extend to discussions about prison rape or safe sexual practices, artistic images that include nude subjects, and arguably the card catalogue of the Carnegie Library. Given that existing technology does not permit material to be restricted to particular communities, online speakers cannot prevent content from entering a geographic community nor prevent users from certain communities from accessing their site.

In summary, the community standard, combined with the difficulty in zoning Internet into specific communities, implies that communication complying with CDA would be restricted, not only to expressions suitable for minors, but to expressions where the level of "decency" would be acceptable for the community most likely to be offended by the message. This would not be proportionate to the legitimate aim pursued.

In assessing the proportionality of CDA, the Court states that due to the breadth of the restriction on speech, the Acts impose an especially heavy burden on the Government to explain why a less restrictive provision would not be as effective. In addressing the issue of possible tagging of "indecent" material, the Court mentions the development of filter Software - especially the PICS.The Court stresses that until a majority of sites have been rated by a PICS rating service, PICS will function as a "positive" rating system, in which only those sites that have been rated will be displayed using PICS compatible software. This means that the PICS standard will function as an information inclusion list rather than an exclusion list thus only site, which have a PICS rating for appropriate content will be accessible, while non-rated sites will be blocked. This type of positive rating is thereby restricting minors' access to a majority of content on Internet, including material of artistic or educational value. The Court also mentions various type of stand-alone software intended to enable parents and other adults to limit the Internet access of children, such as Cyber Patrol68, Cyber sitter, Net Nanny, and Surf watch.

The Court on COPA also considered parental blocking or filtering as a less restrictive means and went a bit further than the Supreme Court. The Court on COPA acknowledged that, while filter software is both over and under inclusive in the breadth of the material that it blocks, it is likely to be as effective as COPA, while imposing fewer constitutional burdens on free speech.

The issue of cyber assemblies exemplified by Jubii and AOL touches the very core of cyberspace being a public, private and commercial sphere, but managed by private parties. Currently, they are services provided for in the commercial sphere of cyberspace connected to commercial content providers. Since they are privately managed, it implies a legitimate right to subject the services to restrictions; for instance by automatically altering expressions such as "click" or "whore" in order to secure a "clean" environment. AOL and Jubii are commercial parties, and they have a legitimate right to regulate according to the codes of their system. Or do they? It all depends on whether we apply a system or lifeworld perspective.

REFERENCES

[1] http://www.cyber-rights.org/reports/governan.htm | [2] http://www.cvhercity.dk/kundeservice/retningslinjer/ | [3] http://courses.cs.vt.edu/cs3604/lib/Censorship/notes.html | [4] http://cyber.law.harvard.edu/ilaw/Speech | [5] http://www.article19.org | [6] http://groups.aol.com/_pub/guidelines.adp | [7] Habermas. J. The Theory of communicative Action, volume to. Oxford. Polity Press. 1992. | [8] Article 19. Draft Cyber Crime Law of Brazil, January 2012

Volume : 2 | Issue : 7 | July 2013 • ISSN No 2277 - 8160

Research Paper | Computer Science

Cyber Crime : How Distributed Denial of Service Works

Santosh Mishra Research Student of Pacific University, Under the guidance of Dr. Ashok Gaekwad

ABSTRACT

A denial of service is characterized by an explicit attempt by an attacker to prevent legitimate users from using resources. An attacker may attempt to: "flood" a network and thus reduce a legitimate user's bandwidth, prevent access to a service, or disrupt service to a specific system or a user. We describe methods and techniques used in denial of service attacks, and we list possible defences. In Recently many prominent web sites face so called Distributed Denial of Service Attacks (DDoS). While former security threats could be faced by a tight security policy and active measures like using firewalls, vendor patches etc. these DDoS are new in such way that there is no completely satisfying protection. We find that under persistent denial of service attacks, class based queuing algorithms can guarantee bandwidth for certain classes of input flows.

KEYWORDS : DOS, DDOS

INTRODUCTION:

A typical DDoS attack is an malicious behaviour to make a computer resource unavailable to its intended users. Perpetrator of DDoS attacks typically focus on sites or services on high-profile web servers such as banks and credit card payment. In a DDoS attack, the perpetrator uses a network of compromised computers, known as "zombies", to send tremendous data to the target(s) of the attack. "Bots" is a kind of software that invisibly infiltrates a computer without the owner's awareness. "Zombie" are the computers that have been contaminated by "bots", who can take over "zombie" computers secretly. Therefore, the owners of "zombies" have no idea that their computers have already become minions of the moon for a malicious force. The only indication of "zombies" for the owner might be just that the running speed is a little slower than usual, but for a common user, not a master of computer science, it's difficult to smell some big serious problem based on this kind of tiny difference.

2. CLASSIFICATION OF DOS AND DDOS ATTACKS

2.1 Attack scenario :

A denial of service attack is characterized by an explicit attempt by an attacker to prevent legitimate users of a service from using the desired resources. Examples of denial of service attacks include :

- attempts to "flood" a network, thereby preventing legitimate network traffic.
- attempts to disrupt connections between two machines, 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.

By using a control master program, the real attacker can stay behind the scenes of the attack. The following steps take place during a distributed attack :

1. The real attacker sends an "execute" message to the control master program.
2. The control master program receives the "execute" message and propagates the command to the attack daemons under its control.
3. Upon receiving the attack command, the attack daemons begin the attack on the victim.

The attacker must study the target's network topology and search for bottlenecks and vulnerabilities that can be exploited during the attack. Because of the use of attack daemons and control master programs, the real attacker is not directly involved during the attack, which makes it difficult to trace who spawned the attack.

2.1.1 System attacked:

Our first category is the system under attack. We can identify a number of attack points that would render the web server useless to normal clients.

A first reasonable attack point for a cracker wanting to launch a DoS is the router that connects the site hosting the web server to its ISP. This would effectively cut off all access to the website.

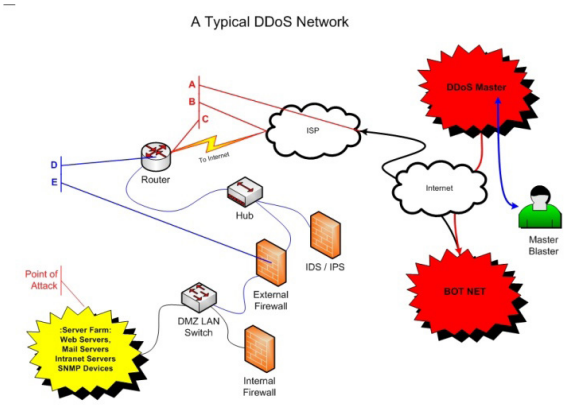
Another possible target is the firewall system, although firewalls usually tend to be (or at least should be) quite immune to direct attacks. On the other hand, the firewall is usually a bottleneck as all in and outbound traffic needs to pass through it. An attack form with a very high load might stop the firewall from working properly. As an example some misconfigured SYN flood attack overload the firewall and blocked most in- and outgoing traffic.

There may be supporting services like database servers etc. As foreign access to these servers should be blocked at the firewall, the chance of a direct DoS attack on one of this systems is fairly small.

2.1.2 Parts of systems attacked:

Some attacks may affect the hardware of a given system although such incidents are very rare. Theoretically, a network card or CPU could fail to work due to some data in a network packet it receives or processes. On the other hand, a simple overload of a 10 MBit/s Ethernet

link is an attack based on the limitation of the hardware. Attacks targeting the operating system or the TCP/IP stack of a host or router are more likely. Many attacks of this type are known, some are bugs that can be fixed, some are fundamental limitations of a protocol specification etc. On the application level there are web servers, database servers, CGI scripts etc. These could be attacked as well.



2.1.3 Bug or Overload:

In general one has to distinguish whether a DoS is a cause of a specific bug or just an overload of components that function according to their specification. Although bugs are often more severe in their effects, most of the time the vendors quickly provide fixes. All the administrators have to do is to apply them to their system in order to avoid fur-

ther attacks. Attacks that are based on an overload are typically harder to cope with. Of course you can buy new hardware, but as long as an attacker finds enough resources to use as relays in the Internet he will always bring your system to a halt. Changing the specification or protocols in order to fix the hole that allows the DoS is nearly impossible as this would often mean changing the software in millions of computers worldwide.

2.1.3 Examples :
The following examples give a little insight in different DoS attack forms. They show that our categorization is suitable for distinguishing common DoS attacks.

Cisco 7xxx routers with IOS/700 Software Version 4.1(1) or 4.1(2) have a bug where a long password given at a telnet login session leads to a buffer overflow and a subsequent reboot. According to our criteria the attacked system is a router, the part of the system under attack is the operating system and it is a bug which has been fixed in subsequent releases.

Jolt2 is an attack targeting most Microsoft Windows systems (Win 98, NT4 SP5 and SP6, Win 2000). Jolt sends a continuous stream of ICMP ECHO REPLY fragments with specially tuned fragmentation parameters to the attacked host. The exact cause of the following action is not known as the code of Microsoft's Operating Systems isn't freely available. What can be observed is that the consumption of CPU and memory resources raises to 100% which renders the system is unusable. This may be used as an attack on web servers, load balancers or even firewalls, if they run one of the named operating systems. The attacks aim at the network stack of the operating system and the reaction is caused by a bug. Fixes are available from Microsoft.

Microsoft's Internet Information Server versions 4.0 and 5.0 suffered from a so called server URL parsing bug. The decoding of escape sequences in URL strings was implemented very inefficiently. Submitting long strings with large amounts of escape characters effectively stopped the web server from working for a significant time. This attack is an attack against the web server application. It is based on an implementation bug. A fix is available from Microsoft.

2.2Methods of Denial of Service Attacks
Some widely known basic denial of service attack methods that are employed by the attack daemons.

2.2.1 Smurf attack: Smurf attacks use so-called amplifier sites in order to multiply the amount of traffic that hits the destination. These attacks send ICMP ECHO REQUEST packets with a spoofed sender address to one or several subnet broadcast addresses. The packets are received and replied by as many stations as are connected to the subnet. The replies are sent directly to the spoofed address of the attack destination. Normally this leads to congestion in the target's local network connection. Often even the lines of the ISP to which the target is connected become overloaded. This attack class strikes all kinds of targets, no matter if routers or hosts. Most of the time it is used against web servers. The effects of the attack typically put a huge stress on the network and the system (both software and hardware) that has to parse and discard the incoming packets. It is not based on a bug, although many people today think that subnets that allow a broadcast ping are a faulty configuration.

2.2.2 SYN Flood attack: It is also known as the Transmission Control Protocol (TCP) SYN attack, and is based on exploiting the standard TCP three–way handshake. The TCP three-way handshake requires a three-packet exchange to be performed before a client can officially use the service. A server, upon receiving an initial SYN (synchronize/start) request from a client, sends back a SYN/ACK (synchronize/acknowledge) packet and waits for the client to send the final ACK (acknowledge). However, it is possible to send a barrage of initial SYN's without sending the corresponding ACK's, essentially leaving the server waiting for the non-existent ACK's. Considering that the server only has a limited buffer queue for new connections, SYN Flood results in the server being unable to process other incoming connections as the queue gets overloaded.

The main principle of SYN flood attacks is to generate many half-open TCP connections by sending SYN packets to the target without replying to the following SYN-ACK packet. Most of the time the SYN packets also have spoofed source addresses of non-existent or currently inactive hosts. As today's hosts can typically handle only a limited number of half-open connections per port and discard new connection requests as long as the so called backlog queue is full, this effectively stops ordinary clients from connecting to the (web-) server. This attack form falls in the category of attacks to web servers or load-balancers which have a weakness in their TCP implementations. Part of the problem is the unlucky connection establishment procedure of the TCP protocol so it is not totally clear, weather it is an implementation bug or design.

2.2.3 UDP Flood attack: It is based on UDP echo and character generator services provided by most computers on a network. The attacker uses forged UDP packets to connect the echo service on one machine to the character generator (chargen) service on another machine. The result is that the two services consume all available network bandwidth between the machines as they exchange characters between themselves. A variation of this attack called ICMP Flood, floods a machine with ICMP packets instead of UDP packets.

2.2.4 Apache MIME flooding: There had been a number of attacks on apache web servers or Apache Sioux Attack With specially formatted HTTP requests it was possible to make the web server use up huge amounts of memory. As soon as the system started swapping out server processes or used up the whole system memory, the server was effectively dead. These attacks both target a specific web server software on the web server systems. They exploit implementation bugs.

2.3From DoS to DDoS
Major Internet websites like amazon or Yahoo tend to have Internet connections with very large bandwidth and server farms with lots of components. Furthermore they are typically protected by firewall systems that block the known attacks that are based on malformed packets like jolt2 does. The architecture of these tools is very similar and in fact some tools are modifications of others. The actual attack is carried out by so called daemons. A number of daemons is controlled by a handler and finally these handlers are activated by the attacker using client tools. The intrusion into computers onto which handlers and daemons are to be installed usually follows a simple pattern:

- A stolen account is set up as a repository for precompiled versions of scanning tools, attack (i.e. buffer overrun exploit) tools, root kits and sniffers, DDoS handler and daemon programs, lists of vulnerable and previously compromised hosts, etc.
- A scan is performed on large ranges of network blocks to identify potential targets. Targets would include systems running various services known to have remotely exploitable buffer overflow security bugs, such as wu-ftpd, RPC services for "cmsd", "statd", "ttdbserverd", "amd", etc.
- A list of vulnerable systems is then used to create a script that performs the exploit, sets up a command shell running under the root account that listens on a TCP port and connects to this port to confirm the success of the exploit.
- From this list of compromised systems, subsets with the desired architecture are chosen for the Trinoo network. Precompiled binaries of the DDoS daemons and handlers programs are created and stored on a stolen account somewhere on the Internet.
- A script is then run which takes this list of "owned" systems and produces yet another script to automate the installation process, running each installation in the background for maximum multitasking. The result of this automation is the ability for attackers to set up the denial of service network in a very short time frame and on widely dispersed systems whose true owners often don't even realize the attack.
- Optionally, a "root kit" is installed on the system to hide the presence of programs, files, and network connections. This is more important on the handler system, since these systems are the keys to the DDoS attack network.

2.3.1 Trinoo: It uses TCP to communicate between the attacker and the control master program. The master program communicates with the attack daemons using UDP packets. Trinoo's attack daemons implement UDP Flood attacks against the target victim.

2.3.2 Tribe Flood Network (TFN): It uses a command line interface to communicate between the attacker and the control master program.

Communication between the control master and attack daemons is done via ICMP echo reply packets. TFN's attack daemons implement Smurf, SYN Flood, UDP Flood, and ICMP Flood attacks.

Stacheldraht: It is based on the TFN attack. However, unlike TFN, Stacheldraht uses an encrypted TCP connection for communication between the attacker and master control program. Communication between the master control program and attack daemons is conducted using TCP and ICMP, and involves an automatic update technique for the attack daemons. The attack daemons for Stacheldraht implement Smurf, SYN Flood, UDP Flood, and ICMP Flood attacks.

Shaft: It is modelled after Trinoo. Communication between the control master program and attack daemons is achieved using UDP packets. The control master program and the attacker communicate via a simple TCP telnet connection. A distinctive feature of Shaft is the ability to switch control master servers and ports in real time, hence making detection by intrusion detection tools difficult.

3. DEFENCES AGAINST ATTACKS

Many observers have stated that there are currently no successful defences against a fully distributed denial of service attack. This may be true. Nevertheless, there are numerous safety measures that a host or network can perform to make the network and neighbouring networks more secure.

To provide protection from DoS or DDoS attacks, basic security measures are mandatory. If a running system is hacked into, no more network attacks are necessary, since local attacks (like processes consuming lots of memory or CPU time, or simply shutting down the system) are far more effective. A set of firewalls should be used to separate the interior net from the Internet.

These measures include:

3.1 Filtering Routers: Filtering all packets entering and leaving the network protects the network from attacks conducted from neighbouring networks, and prevents the network itself from being an unaware attacker. This measure requires installing ingress and egress packet filters on all routers.

3.2 Disabling IP Broadcasts: By disabling IP broadcasts, host computers can no longer be used as amplifiers in ICMP Flood and Smurf attacks. However, to defend against this attack, all neighbouring networks need to disable IP broadcasts.

3.3 Applying Security Patches: To guard against denial of service attacks, host computers must be updated with the latest security patches and techniques. For example, in the case of the SYN Flood attack, there are three steps that the host computers can take to guard themselves from attacks:

- increase the size of the connection queue,
- decrease the time-out waiting for the three-way handshake,
- and employ vendor software patches to detect and circumvent the problem.

3.4 Disabling Unused Services: If UDP echo or chargen services are not required, disabling them will help to defend against the attack. In general, if network services are unneeded or unused, the services should be disabled to prevent tampering and attacks.

3.5 Performing Intrusion Detection: By performing intrusion detection, a host computer and network are guarded against being a source for an attack, as while as being a victim of an attack. Network monitoring is a very good pre-emptive way of guarding against denial of service attacks. By monitoring traffic patterns, a network can determine when it is under attack, and can take the required steps to defend itself. By inspecting host systems, a host can also prevent it from hosting an attack on another network.

It should be used to notify the system administrators of unusual activities. The firewall rules should include some sanity checks for source and destination addresses: Packets arriving from the Internet must not have a source address originating from the interior net, and vice versa. By rejecting packets from the interior net with a non-local source address, packet spoofing becomes impossible. This technique is known as ingress and egress filtering. Even if a host is invaded by a hacker, these rules make it impossible to use that host as a platform for further attacks requiring spoofed packets (e. g. SYN-Floods, Smurf-Attacks, etc.).

3.6 Use of balance loader: It is rather difficult to defend against DoS or DDoS attacks which overload the systems network connection or local resources. These attacks usually put a heavy load on the target by making regular requests very rapidly.

It is hard to distinguish if a web server is stormed by thousands of clients, or if there is a DoS attack in progress. A simple way to force the problem of heavy load is to use a server farm together with a load balancer. This will help against small attacks, but not against a DDoS started from several hundred hosts. Furthermore, increasing the number of servers is rather expensive.

Many experts think that the only durable solution to this problem is to globally improve the security on all hosts in the Internet to take attackers the possibility to use other hosts for running daemons. This includes securing the local operating system, applying ingress- and egress filters and protecting sites with firewall systems.

3.7 First packet rejection: A simple response to SYN floods is the "first packet reject" method: The first packet sent by every host is discarded. This renders the common SYN flood attack ineffective, but all normal connection requests are delayed to the first retransmit of the SYN packet. Thus, all requests will be considerably slower. On the other hand, the SYN flood attack may be simply adapted by sending each SYN packet twice.

3.8 Moving target defence: Another technique is the so called moving target defence. Here the host under attack changes its IP address to avoid being attacked. The problem here is that the legitimate users of the system need to be informed that the IP address has changed which usually is done by updating the DNS system. Due to caching it can take up to a number of days until all clients are informed of the update. This is clearly unacceptable as the effects are as severe as any DoS attack can be. Furthermore attackers only need to incorporate DNS lookups into their tools in order to evade this protection.

REFERENCES

1. K. Hafner, M.Lyon. Where Wizards Stay Up Late.Simon & Schuster, New York, 1996. | 2. E.H. Spa_ord. The internet worm program: Ananalysis. Purdue Technical Report CSD-TR-823,Deoartment of Computer Sciences Purdue University,West Lafayette, IN. 1988. | 3. D. Seeley. A tour of the worm. Department of Computer Science, University of Utah, 1988. | 4. M. Eichin, J. Rochlis. With microscope and tweezers: An analysis of the internet virus of november 1988. Massachusetts Institute of Technology, 1988. | 5. http://www.nwfusion.com/news/2000/0209attack.html | 6. L. Stein. The world wide web security faq, version 2.0.1. http://www.w3.org/Security/Faq/ | 7. S.M Bellovin, W.R. Cheswick. Firewalls and Internet Security. Addison Wesley Longman, 1994. | 8. Dr. J.D. Howard. An analysis of security incidents on the internet 1989 - 1995. Carnegie Mellon University, Carnegie Institute of Technology,