DENIAL-OF-SERVICE & DISTRIBUTED DENIAL-OF-SERVICE ON THE INTERNET

K. Ormiston[1] and MM Eloff[2]

[1]Business Connexion, [2]School of Computing, UNISA

[1]kate.ormiston@bcx.co.za, [2]eloffmm@unisa.ac.za

[1]PO Box 1252, Midrand, 1685, South Africa. Tel: +27 11 266 1062,

[2] School of Computing, UNISA, Pretoria, 0003, South Africa. Tel: +27 12 429 6336,

ABSTRACT

Denial-of-Service and Distributed Denial-of-Service is costing the economy world-wide billions of dollars. The economy is the cornerstone of our society and its collapse will certainly change the way in which humanity exists today. The three main goals of computer security are availability, confidentiality and integrity. The focus of this paper is on attacks that compromise the availability of systems.

A Denial-of-Service attack is a very serious threat to the infrastructure of the Internet, as well as its users. The Internet plays an important role in our everyday lives and many companies are dependent on it to conduct business or provide critical real-time services and cannot function when computer systems and network access go down. When a company cannot offer its services it will lose money, its reputation and ultimately clients. This in turn will impact the economy and eventually all of us. This is the major driver for network security requirements.

In order to prevent these attacks from happening we need to understand what exactly the terms Denial-of-Service and Distributed Denial-of-Service mean and how they effect or impact the economy. This paper is a summary of a literature study, with regards to the causes and effects of these attacks, as well as potential solutions to the problem.

KEY WORDS

Denial-of-service; distributed denial-of-service; security; availability; social engineering; e-mail; internet; attack trends; defense.

DENIAL-OF-SERVICE & DISTRIBUTED DENIAL-OF-SERVICE

ON THE INTERNET

1. INTRODUCTION

Denial-of-Service and Distributed Denial-of-Service is costing the economy world-wide billions of dollars. The economy is the cornerstone of our society and its collapse will certainly change the way in which humanity exists today. The three main goals of computer security are availability, confidentiality and integrity. The focus of this paper is on attacks that compromise the availability of systems. Availability means that when an authorized entity wishes to access an asset at an appropriate time, it will not be denied. A Denial-of-Service attack is a very serious threat to the infrastructure of the Internet, as well as organizations and all end users. The Internet plays an extremely important role in our everyday lives and many companies are dependent on the Internet to conduct their business and provide critical real-time services. Many companies cannot function when computer systems and network access go down.

When a business cannot offer its services then it will lose money, its reputation and ultimately clients, this in turn will impact the economy and eventually all of us. This is the major driver for network security requirements.

The remainder of the paper is structured as follows: Section 2 contains an overview of Denial-of-Service (DoS) and distributed Denial-of-Service (DDoS), followed by a discussion of the evolution of DoS and DDoS. Section 4 contains a taxonomy of DoS and DDoS attacks with a discussion of Solutions in the 5th section and Solution implementations in Section 6. The paper concludes in the last section.

2. OVERVIEW OF DENIAL-OF-SERVICE AND DISTRIBUTED DENIAL-OF-SERVICE

During a Denial-of-Service attack the victim's normal service offering will be unavailable or perhaps too slow to be used by legitimate users. When a Denial-of-Service attack occurs, the system is flooded with unwanted information and becomes overwhelmed to a point that it can no longer function. The target is the systems resources namely bandwidth, processing power and storage capacity. These become consumed making the system unavailable, and therefore Denial-of-Service can sometimes be called an availability attack. It can also be classified as logic attacks which exploit known vulnerabilities causing a crash or reduction in performance.

A Denial-of-Service attack is distributed by using 'innocent computers' also known as Zombies, found at different locations, to launch multiple attacks on a chosen final target. This attack is performed in 2 phases, see Figure 1; first they use an attack to place a Trojan horse file, which offers a backdoor to a system, on any number of target 'Zombie' machines by using an e-mail attachment or exploiting a buffer overflow. Then the final victim/s is/are chosen and signals sent to all the zombies to attack at the same time.

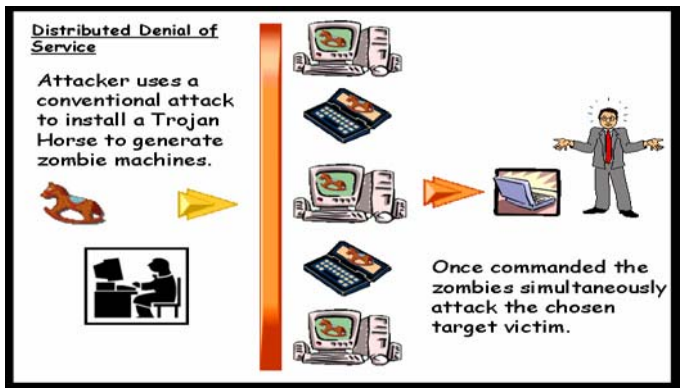

Figure 1 Distributed Denial-of-Service Attack Method

One of the main differences between Denial-of-Service and Distributed Denial-of-Service attack is the source of the attack; Denial-of-Service has a single source, whereas Distributed Denial-of-Service uses multiple sources [SANS, 2005]. These multiple sources, called 'Zombies' or 'Bots' are broken into and controlled to perform malicious activities. An attack can therefore be performed using many levels of communication. Denial-of-Service is essentially a single 1-tier attack that has a single communication line between attacker and victim, whereas Distributed Denial-of-Service attacks can be 2-tier or 3-tier.

A 2-tier distributed denial-of-service attack has a wall or layer of zombies or bots between the attacker and the victim; this enables the attacker to communicate with his controlled layer, using various methods, and control the attack on the victim. For example, a Smurf attack [SANS, 2000], involves a variation of ping, first the 'reply to' address of the ping is replaced (spoofed) with the victims and then the ping is broadcast by the attacker to everyone on the network. Once everyone replies to the ping the victim is flooded.

Generating a 'master' computer that in turn manages the 'handler' or 'slave' machines, generates a 3-tier distributed denial-of-service attack. This is a very common model for current distributed denial-of-service attacks including: TrinOO, Tribal Flood Network (TFN), Stacheldraht "Barbed Wire", and Shaft and TFN2K. There are two popular types of DDoS architecture models namely Agent-Handler and IRC-Based [Cisco, 2005]. They work the same way except in the IRC-Based model an attacker uses the IRC (Internet Relay Chat) ports for sending commands to agents instead of a programmed 'handler' machine. The IRC method allows for greater anonymity for the attacker and agents, who simply listen on the channel for any commands.

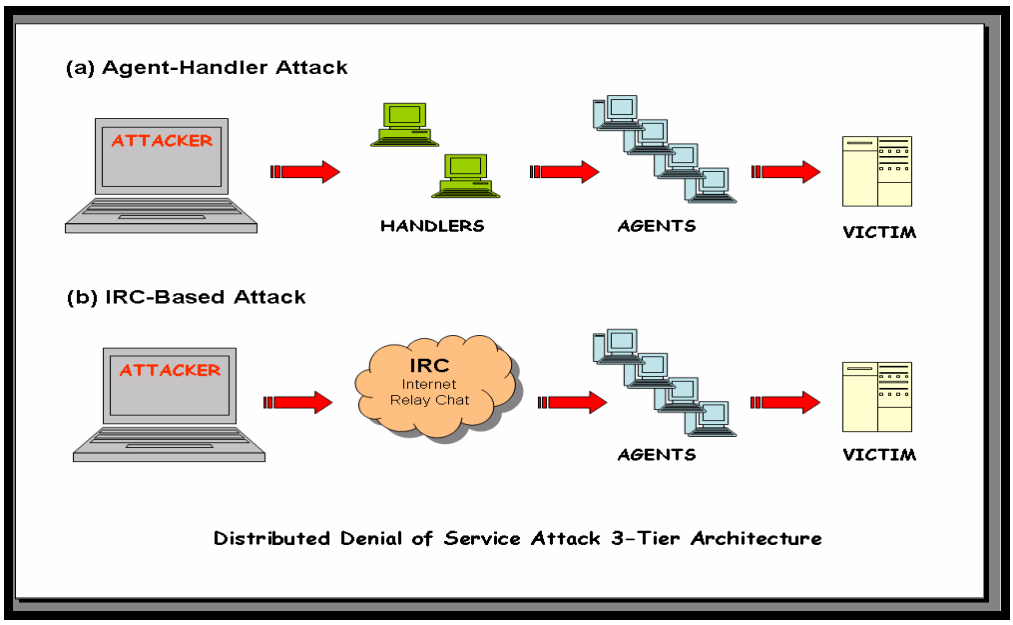

Figure 2 Distributed Denial-of-Service Attack Architecture

When using distributed techniques such as 2- or 3-tier, as shown in figure 2, one can attack much more powerful system servers. This is because the attacker can multiply the resources on the attacking end. A normal Denial-of-Service has to comply with the rule that the targets' resources must be less than that of the agent used to perpetrate the attack. When a single agent is used, action can be taken to prevent the traffic but with multiple agents one would have to co-ordinate a much larger effort.

The agents may also be widely spread on the Internet and unable to detect any differences between legitimate and attack traffic. While under a Denial-of-Service attack it is possible to add more resources to cope with the unwanted traffic and prevent damage, however this is not realistically possible under a Distributed Denial-of-Service attack were the number of agents used can be increased with ease. Traceback of attack traffic also becomes more difficult as the levels of communication in the attack network or 'botnet' increase.

Distributed Denial-of-Service attack sizes can be measured by the following characteristics: amount of traffic generated, number of participating sites and also the duration of the attack [Cisco, 2005]. The attacker has no limit to what he can generate; all he needs is the ability to compromise remote sites. The reason they are so powerful is because of the multiplicative effect of the two- or three-stage attack. The victim must defend itself against n attacks from n zombies all acting at once, instead of one Denial-of-Service attack from one malicious host. Another major advantage for the attacker is that it is easy to launch these attacks through the use of scripts, freely available on the web.

3. EVOLUTION OF DENIAL-OF-SERVICE & DISTRIBTED DENIAL-OF-SERVICE

Malware is short for malicious software and is code that generates an attack to exploit our resources. Trojan horses, Viruses, Worms and spyware are often used to refer to malware. A Trojan horse is a program that overtly does one thing while covertly doing another, according to Pfleeger & Pfleeger [2003]. Viruses, types of a Trojan horse, have been reported since the early 1980's and are self-replicating programs made up of malicious code. They spread by attaching themselves to other programs or operating systems and may carry destructive payloads that can be

activated through various means, e.g. by a request from the program they are attached to. All viruses require a host program that can execute in order to run their code.

The first major Internet worm, '88 RTM Internet Worm', was released by Robert T. Morris in 1988 [SANS, 2000]. A worm is similar to a virus in that it is also a self-replicating program that attaches itself to executable programs, but it does not require the host to propagate, as it is self-contained. Self-propagating worms are now common thanks to automated tools. Worms are able to locate vulnerable machines and infect them with a copy of its code. Once they have an army of infected machines they will be able to launch a Distributed Denial-of-Service attacks using its code. Code Red, Code Red II and Sasser are all examples of worms that can infect hundreds of thousands of machines and make them sources of attack. More recently we have Mytob and its many variants and Fanbot, Bagle and Bayfraud. Viruses and worms have become a concern in large organizations as this usually means downtime [Garvey, 2005]. Systems need to be offline in order to perform the time-consuming and costly upgrades.

When analyzing past attack mechanisms it clearly shows an increasing level of attack tool sophistication. Internet usage has boomed in the past 5 years and the first Internet measurement study, which was conducted in 2001, indicated a low estimate of 4000 attacks per week. According to Arbor's special report [2005] the size and frequency of attacks have increased dramatically. The first Denial-of-Service technology used simple tools to generate and send packets from a single source to a single target destination. These days the technology can perform single source attacks against multiple targets, multiple source attacks against multiple targets and multiple source attacks against single targets. They use layers of zombies as a hierarchy to increase the levels between the attacker and victim, this makes tracing them more difficult. The processing power of the entire zombie network can be used in the attack.

Freely available attack tools are fully functional, pre-compiled and sophisticated enough to launch a large scale attack. The slammer worm managed to infect 90% of the vulnerable hosts within 10 minutes of its release and had a replication rate of 8.5 seconds [Cisco, 2005]. Reports have shown the worm's payload is not as destructive as the network congestion they cause. Service providers will need to assist in mitigating these types of attacks because nowadays we need a few minutes reaction time instead of days. We may only have a few seconds in the near future.

Although the largest botnet identified during an attack using measurement and detection tools, contained only 20,000 hosts, 100,000-zombie networks have been reported. The armies are used for extortion, identity theft and credit card fraud. Reports of 'Bot-Wars' between hackers show their military intelligence as they fight to gain control of these valuable assets, by writing code that removes their competitors, until they control the largest army [AINSLIE, 2004].

The time between discovering the vulnerability and wide exploitation has been decreased significantly. Viruses now take advantage of "zero-day exploits", by exploiting weaknesses in the system as soon as the flaw is announced. The use and sophistication of automated attacks have increased, functions now include list creation of compromised and potentially vulnerable hosts and script utilization to automate scanning, exploitation, deployment and propagation. Vulnerabilities in Unix-based systems were the original targets for automated attacks; social engineering was required for Windows-based systems but this is no more the case.

Distributed Denial-of-Service networks are more difficult to identify now due to the use of IRC networks and protocols as these allow outbound connections to a standard service by a legitimate network service to control a group of Distributed Denial-of-Service agents. Large traffic is common for these communication channels and an attack may go unnoticed. The IRC server also assists the attacker by maintaining a list of agents that are currently available. The attacker can log on to the IRC server which receives this information from notifications via the IRC network software [CERT, 2001].

In order to protect systems and networks against Denial-of-Service and Distributed Denial-of-Service attacks, we need to apply different approaches depending on the types of attack being used. This is the problem, we can protect against existing methods by analysis of past attacks, but we have no idea what new vulnerabilities come into play as the Internet continues to grow. There is a vicious circle between attackers and defenders, as expensive changes for dealing with attacks are implemented, attackers are discovering new vulnerabilities and enhancing their tools to bypass these newly secure systems.

4. TAXONOMY OF DOS AND DDOS ATTACKS

4.1 Introduction

Many types of people perform these attacks. 'Script Kiddies' are inexperienced hackers who download attack tools from the web and use them unaltered and they are the source of most attacks, [CERT, 2001]. To some people this is simply a game, the criteria for winning includes best attack code written, the size of the army established, number of targets hit or even the value of their loss. The possibilities are endless and the challenges in stopping this threat are overwhelming. Sophisticated career criminals, even though there are fewer cases, usually cause more damage due to the fact their intention and goal are clear to them. These attackers can usually write their own tools and are able to find the hard drive to reach intelligent resources that can be used in their attacks. You can easily find advertisements in a newspaper or on the web that will enable you to purchase an attack against the target of your choice and this makes every one a potential attacker.

There are many reasons why attackers would want to deny service. These include pranks, showing something can be done (Proof of Concept), recognition, supremacy and even revenge. There have been recent reports of their use in electronic protests showing an attacker's personal or political position on an issue. Competition in the market place may lead to many types of malicious activities, for example to stop a web site offering services to its customers in order to make them look bad and gain a higher market share. Extortion is definitely on the rise; many companies are bribed for money, especially if there is a time limit involved. It is common for a betting site to be taken down and demands made for money in order for them to operate before a crucial big horse race, or international sports event that is about to take place.

The Tumbleweed [2005] says "E-mail has displaced the telephone as the primary means of communication for business. According to IDC thirty billion messages crossed the Internet each day in 2004. The term "Dark Traffic", used to describe unwanted e-mail traffic that flows "under the radar" of traditional e-mail and network security products, makes up 70% of inbound traffic that should not be taken in by a company. E-mail Denial-of-Service attacks, also known as mail bombing or flooding, attempt to overwhelm an e-mail server or relay with a mass of messages. This results in the server rejecting legitimate mail and dropping connections. An attack sends tens, hundreds, or thousands of e-mail messages per second at its target for hours or even days. Agent zombies infected with e-mail viruses, worms and spy-ware are able to launch a Distributed Denial-of-Service attack on one or many victims, because they are controlled remotely by the hacker who sent them. During the past 12 months, 63% of their survey respondents said they had been hit by e-mail Denial-of-Service attacks, over half had multiple attacks. Directory Harvest Attacks are designed to identify valid e-mail addresses, in a domain, for resale or future Spam; this causes a delay of e-mail delivery and can cause e-mail servers to fail [Tumbleweed, 2005].

After reading Pfleeger & Pfleeger [2003], it is easy to understand why the Internet is so vulnerable when it is made up of networks of networks; in fact it is an enormous, heterogeneous, physically and logically exposed Federation. The attacker can be geographically anywhere, anonymity is on their side, there are millions of points that can be used for both origins of an attack and targets, and the paths between hosts are unknown. The large amount of sharing, unknown perimeter and shear size and complexity of the Internet make it impossible to secure in its entirety.

The Internet is an infrastructure of interconnected systems and networks each with their own interdependent security, if any at all. Those systems with unprotected assets will be used to attack the rest of the global Internet. Your systems susceptibility to Denial-of-Service attacks is dependent on the state of security of all systems connected to the Internet. There are also a limited number of resources that are consumable on the Internet; the tools used today can disrupt even the most abundant of them. According to Ainslie [2005] there are 3 primary vulnerabilities in the way the Internet works, which are exploited. The first is a weakness in the Transmission Control Protocol (TCP); this is the standard connection oriented host-to-host protocol used over packet switching networks. It is used in a SYN flood attack when the machine cannot process the TCP connection requests fast enough. The second lies in the User Datagram Protocol (UDP), a stateless protocol offering direct datagram communication, which sits on top of IP networks, like TCP, except with less error recovery services. It is mainly used to broadcast messages and therefore flooding. The last aspect to the Denial-of-Service attacks is the concept of application protocol abuse. In fact, Denial-of-Service attacks travel across many Internet protocols, including HTTP, IM, FTP, RPC, etc.

The "Anna Kournikova" e-mail virus [CERT, 2001], relied on the human's fascination with celebrities. They opened it and thus it spread to millions of user's worldwide. End users are not technically competent nor do they have the security knowledge to protect themselves against attacks. People with malicious intent use this fact to their advantage by directing their attacks at unknowing victims. They try to persuade the victim to be helpful in the attack by revealing security information, or by using social skills or even with personal interaction. This reliance on human nature is known as social engineering and makes the attacker's job a lot easier,

4.2 Taxonomy of attacks

In order to understand all of the different types of attacks we need a way to classify them according to various properties. There have been a number of taxonomies proposed over the years to assist researchers in analysis of past, current and future trends of attack and defense mechanisms, as summarized in Table 1.

SANS [2003] classified Denial-of-Service attacks as resource exhaustion flooding attacks and logic attacks. Logic attacks can cause a server or service to degrade or crash by exploiting security vulnerabilities and the flooding attack consumes the network or servers resources with unwanted traffic until it degrades or stops responding. Their paper divides these flooding attacks into 9 categories. The first is the simplest, Direct Flooding Attacks, a 1-tier attacker to victim flood, and using protocols such as ICMP, UDP and TCP. Then using Remote Controlled Network Attacks, an attacker, through the use of zombies, can launch direct flooding or reflective attacks.

Reflective attacks use the victims IP address as a source address in packets, sent to intermediary hosts, which means they will receive all replies and the attacker will remain anonymous. These attacks can be further divided into Smurf and Fraggle Attacks, ICMP, TCP SYN, UDP, TTL Expiration and DRDoS attacks. The fourth category is Worms, then Viruses, followed by Protocol Violation Attacks, Fragmentation Attacks, Network Infrastructure and Other. The categories certainly increased my understanding but these days a single attack is usually made up of a majority of the above categories.

Table 1: Attack Classifications

ATTACK CLASSIFICATIONS			
Hussain, et al [2003]	**SANS [2003]**	**Mirkovic, et al [2004]**	**Specht, et al [2004]**
Flooding:	Direct Flooding (1 tier)	Degree of automation	Bandwidth Depletion:
Single Source	Remote Controlled Direct Attack	Exploited Weakness	Flood
Multi Source	Remote Controlled Reflective	Source Address Validity	Amplification
Reflected	Worms	Characterization possibility	Resource Depletion:
	Viruses	Attack Rate Dynamics	Protocol Exploit
	Protocol Violation	Impact on Victim	Malformed Packet attack
	Fragmentation	Victim Type	
	Network Infrastructure	Agent Set Persistence	
	Other		

Hussain, et al [2003], use header analysis, ramp up behavior and spectral analysis in the case of spoofing to identify under which of their classes flooding attacks fall. Classifications include (a) single source, (b) multi-source, or (c) reflected, based on the number of attackers and their location, with respect to the observation point and victim.

Mirkovic & Reiher [2004] offer a DDoS taxonomy based on analysis of the two phases of the attack, they call the first the *recruit, exploit and infect* phase which describe the strategy for preparing the attack network. The second phase analyzes the characteristics of the attack itself, this is the *use* phase. They also take into account the effect of an attack on the victim. These classifications are discussed in more detail in my full paper, see references.

Specht, et al [2004] only divide their attack taxonomy according to the effect on the victim, either bandwidth or resource depletion. If the victim's bandwidth is flooded with attack traffic, the normal traffic cannot get through even though the system is available to process requests. The taxonomy includes examples of Flooding Attacks: UDP and ICMP Floods and Amplification (Reflection) Attacks: Smurf and Fraggle. The Resource depletion effect will leave the systems with too many illegitimate requests caused by the sending of malformed packets or exploitation of Internet Protocols. The system cannot process the true requests during this time or worse, it can crash again. This analysis is based on the cause of service denial, an interesting perspective.

By using the above taxonomies we will be able to critically analyze characteristics of Denial-of-Service and Distributed-Denial-of-Service attacks. Together they have enabled us to understand the nature and scope of the problem in a much greater depth.

4.3 Difficulties in Defending

Lack of Security Knowledge*:* Software is written without a thorough understanding of security requirements that need to be met during the design phase of software development projects. Developers need to design platforms independent of user ability and network architecture. Customers frequently choose functionality over security requirements when spending money on IT related projects. Use of the Internet has boomed in recent years leaving a drain in qualified resources in the industry. People who have a varying degree of experience and knowledge are managing systems. The rate at which technology infiltrated our working lives was much faster than our ability to learn how to master their functionality.

Size and Complexity*:* There is no geographical or national boundary and we must work on an international level to solve all these types of problems. The variety of platforms, applications

and protocols in use on the Internet is endless and defense mechanisms are expected to conform to all these differences in software and architecture. The number of users connecting to the Internet increase by the second and many of them will not be protected and therefore a valuable weapon in the attackers hands. Anyone can connect and have access to a variety of attack tools, which evolve rapidly in an open-source environment.

The Law and Anonymity: As the Internet resides across the world it is difficult to prosecute criminals of cybercrime. International Law is complex and investigations rarely lead to a conviction. Attackers use machines called handlers or masters and in some cases machines called stepping stones before the handlers. All these layers of indirection enable the attacker to remain hidden. They can also misuse legitimate services by assuming the identity of a legitimate client by forging the source IP field; this is know as IP spoofing. A reflection attack is an example where an attacker sends requests to a publicly available service and uses the victims' source address causing all server replies to be sent to them. Attackers know that IP Networking assists them in hiding their identities and even if they are revealed, the evidence is usually not sufficient to prosecute. A recent example is the press article in The Register, 16 March 2005, by Jan Libbenga, 'Dutch hackers sentenced for attack on government sites'. This was the first conviction in the Netherlands for this type of attack and was the result of legal proceedings made by the Dutch government against the 15-person hacker group after a 5-day DDoS attack [Libbenga, 2005]. The group's spokesman, an 18-year-old, received a 38-day sentence that he is appealing on grounds of no technical proof. In total 5 of them received sentences such as work orders and youth detention.

5 POSSIBLE SOLUTIONS

5.1 Taxonomy of Defence

This section will briefly introduce the taxonomies of defense proposed by Mirkovic et al [2004] and Specht et al [2004], as per Table 2.

Mirkovic et al [2004] discuss an important point in that when a victim is attacked, a co-coordinated, distributed response is the best defense. We need to join our network forces to detect and respond more efficiently. However, this is where the problems come in because we cannot enforce or guarantee this. We need to police the traffic that travels the Internet and collect information that will enable us to react accordingly. This means we need intelligent systems that communicate efficiently and change dynamically. They offer three classification groups in the proposed defense mechanism taxonomy, based on their activity level (preventative or reactive), deployment location (victim, intermediate or source network) and cooperation degree (Autonomous, cooperative, Interdependent). The paper suggests that network providers start to use dynamic pricing; this is currently a very controversial subject in the business world. Their solutions follow a general attack handling strategy: increase awareness and skills, pro-actively protect and detect and finally react properly during an attack by choosing appropriate mitigation techniques such as traffic dropping or deflection, load balancing and throttling. Most importantly they admit to the need to keep all post-attack forensic analysis, not only to detect and prevent repetition, but to assist law enforcement and to make insurance claims in the case of damage. They proposed only partial solutions to these attacks and agreed that further research is definitely required.

Specht et al [2004] offer three categories of countermeasures which essentially represent pre-attack detection and prevention, stopping or mitigating a current attack and post-attack network forensics. Their solutions also follow the general attack strategy: increase awareness and skills, pro-actively protect and detect and finally react properly during an attack by choosing appropriate mitigation techniques such as traffic dropping or deflection, load balancing and throttling. Most importantly is the awareness of the need to keep all post-attack forensic analysis, not only to ensure a repetition is prevented, but to assist law enforcement and to make insurance claims in the case of

damage. They proposed only partial solutions to these attacks and agreed that further research is definitely required.

Table 2 Defense Classifications

DEFENSE CLASSIFICATIONS	
Mirkovic, et al [2004]	**Specht, et al [2004]**
1. Activity Level: ▪ Preventative ▪ Reactive 2. Deployment Location: ▪ Victim ▪ Intermediary ▪ Source 3. Cooperation Degree: ▪ Autonomous ▪ Cooperative ▪ Interdependent	1. Pre-Attack: Detect & Prevent ▪ Handlers or secondary victims ▪ Potential Attacks 2. During: Mitigate/Stop/Deflect: ▪ Load Balancing ▪ Throttling ▪ Drop Requests 3. Post Attack Forensics: ▪ Traffic Analysis ▪ Event Logs ▪ Traceback

Various defense taxonomies have enabled the generation of solutions that cover a multitude of attack methods using a combination of very specific and more general strategies and algorithms. Once we understand attack and defense strategies we will be able to evaluate the solutions according to unique requirements. A determining factor in choosing and implementing a solution is the cost associated; a company needs to get the maximum protection with the least cost. The larger the network the more money you will need to spend protecting it. The more risk associated with a denied service the more budget will be allocated to its continuity.

5.2 Defense Strategy

Awareness & Skills: All users should be aware of the problems caused by these types of attacks. It is a community effort, if you are connected make sure you have security and it is up to date. Be aware of what vulnerabilities are being exploited and whether they affect your system. Education is the key, learn and teach others, become knowledgeable about security. If your business is reliant on large sums of income from a web site, then you should have trained security engineers who understand how to mitigate attacks quickly. As a result of the Morris worm attack in 1988, the CERT/CC (Computer Emergency Response Team) was created, to focus on improving Internet security. The centre is based at the Carnegie Mellon University Software Engineering Institute and is run by Internet Security Experts offering advice, training and free technical documentation. They do on-going research into current intruder activity trends, newly developed malicious code and discovered vulnerabilities and can even assist in response co-ordination. Awareness works both ways, just the same way as you need to be aware of any new problems, so do others. Thus, the number of attacks reported will be significantly lower than the projected number of infected machines involved. Nowadays many tools are sophisticated enough to perform advanced trace-back capabilities that can be used as evidence by law enforcement in order to prosecute attackers.

Detection: The following are signs of DoS and DDoS attacks: Changes in your network (Internet) or computer performance, usually to a slower speed. Very high activity of traffic on the network or flickering lights on your modem. The main detection strategies are signature and anomaly detection and hybrid systems, which combine the two. An automatic intrusion detection system (IDS) will enable you to react quickly during an attack, which may prevent further damage. It can also provide valuable information on the type of attack and steps to be taken. Traffic anomaly detectors are available for large networks. They usually have a base model of normal

network activity against which current states are checked. If unusual or excessive activity occurs, flags can be raised and various steps to mitigate the problems. The base model needs to be updated regularly to remain accurate, as do attack (pattern) signature files.

Reaction/Response: Based on the type of attack, an appropriate response plan should be initiated. These actions may include contacting your ISP, starting contingency plans or performing technical steps to reduce the impact of the attack. Some systems may provide automatic notification enabling you to react quickly, while some may offer automatic reaction to an attack. This reaction can range from contacting a named person by sms or e-mail, or even managing the network during an attack. The important thing is for defense mechanisms to react quickly.

Attack Mitigation: According to dictionary definitions to mitigate means to make the threat less great or severe. We will now discuss three modern strategies.

DDoS diversion systems: Honeypots fall into this class and two types can be used. Low-interaction honeypots emulate services and operating systems which prevent the attacker from interacting with the real system. They are easily discovered because the services cannot provide the attacker with enough detailed information. The other honeypots offer high-interaction, and provided they are not attacked themselves they can raise warning flags when the network is compromised or attacked. A honeynet is an unprotected, standard off-the-shelf architectural network design that attempts to trap attackers and gain valuable information on their motives, tools and methods.

Route Filtering: During an attack Blackhole routing sends the traffic to a null location where it is dumped and Sinkhole routing directs it to a valid IP address for checking. There are many ways to filter traffic, we could use the source address, but this is usually spoofed in an attack, or the filtering of the service if the attack mechanism is known. The destination address can be filtered because the target addresses are usually known. Unfortunately they will lose legitimate traffic too.

Hybrid Methods and Guidelines: The combination of numerous techniques will bring the advantages of each and therefore offer the best mitigation against an attack. The idea is to detect as quickly as possible and notify the attackers where possible to reduce the impact.

Protection & Prevention: Your ability to detect and react to attacks will depend on your preparation and planning. Network design should include detection and prevention mechanisms. Make sure you have insurance in case you suffer a loss. Build relationships with your service providers and for worst case scenarios have contingency and response plans setup.

5.3 Solution Decision Considerations

In this section we will discuss some of the issues that will determine the type of solution implemented to prevent DoS and DDoS attacks from causing damage.

Companies will need to identify what exactly they need to protect and then how much they are willing to spend protecting it. The cost of the solution must be a reflection of the value of the asset it is protecting. If your web server brings in $16 million a day, that is exactly what you will lose should it fail. Therefore, it is definitely worth spending serious money on protecting.

Then there is the issue of liability. Who is liable when these attacks happen? We can trace the secondary victims but not the attacker. Are the secondary victims then responsible? Can the software makers be held liable for vulnerabilities, hardware vendors for intrusions, and service providers for use of their network? If the perpetrators are caught, what penalties do they face for their crimes, what evidence can be provided? The Internet is a place to live and work in virtual reality, it has a huge impact on the living world around us, and yet there are no formal rules and few laws enforced on a global level to control what happens there. If each of us as secondary users is responsible it may cost a fortune to stay connected to the Internet. Apart from the legal and liability

costs should your computer be used in an attack, there would be the need to maintain your system by obtaining the latest hardware, software, daily patches and updates available for download in order to protect yourself against the latest attack. Few companies currently deploy mechanisms at the source network but if secondary victims are held accountable then we will definitely see an increase in the use of these mechanisms. Service Providers charge extra for DoS protection due to the large costs in deploying and maintaining a semi-protected infrastructure.

The last issue is that of skilled personnel. These days companies may have an IT department consisting of a few systems engineers and they may be enthusiasts and perhaps completely up to date on the latest technologies. Some may rely on the networks for defence and even then they may still require the services of experts in the field to implement and maintain the defence mechanisms. Whether you choose to use permanent staff or hire consultants, there is a huge cost involved if you require the best.

These days we are able to easily detect and prevent known Denial-of-Service attacks by enhancing the operating system capabilities and disabling directed broadcasts According to Cisco, [2005]. Distributed Denial-of-Service attacks can be prevented to some extent if popular methods are used for which specialized detection tools exist. If it is a new attack tool, then we rely upon the firewalls and routers to either block, filter or slow down the unwanted traffic. There is ongoing research into IP traceback, identifying the real source of a spoofed packet, to enable victims to find these attackers. Problems with methods of IP traceback: manual methods can be a slow complicated process of logging into each router on the path. Some expensive routers may have processing capabilities with built in software providing some level of automatic IP traceback.

Link testing requires an active attack for the duration of the testing of upstream links until the source is found. Input debugging requires ISP co-operation and management overhead. There are multiple layers in a Distributed Denial-of-Service network, usually made up of innocent victims; the originator may not even be active when the attack occurs. Firewalls can limit the rate of ICMP and/ or SYN packets, check for correct reverse paths, use Ingress/egress filtering (checks packets out, have valid inside source address, and packets in must have outside source destination), and prevent packet delivery from unknown hosts. Router Solutions through software enhancements include sending info to another source or storing info on the destination of packets for later use, and marking them with extra information.

6 SOLUTION IMPLEMENTATION

The need for security will continue to grow and become more critical. Our ability to defend our information assets will depend upon our ability to stay ahead of the game. We need to find vulnerabilities and fix them faster than they can be exploited or to find ways to prevent them in the first place. We need to prevent this “Dark Traffic” and build tools to assist us with accurate detection [Tumbleweed, 2005]. At least we need to know when we have been hit. Now is the time to have a look at the system you use to connect to the Internet. It is important to assess the chances and scale of a possible attack. How reliant is your company on Internet services?

The first task should be to analyze your existing defenses to see what your current security status is. Where do your threats and vulnerabilities lie? Then decide what you need to protect, what assets are valuable, and what you should be protecting them against. Then start doing some of your own research to become more knowledgeable on your exact requirements, this will help you better assess the solutions available to you in the market. There will be many similarities, differences, strengths and weaknesses in the solutions. Their costs and levels of effectiveness will differ. Unless you are willing to pay for professional assistance and trust their work, you will need to do all of the above yourself. If you decide to approach companies regarding a particular solution, remember they are in business to sell, understand your requirements and ensure they are being met. The product should be able to check for IP anomalies and validate fragments, block Ping O’ Death,

Land, and Broadcast and ICMP backwash attacks. It must be able to control all types of floods, record and check for worst offending IP addresses and do inbound port filtering. When choosing a solution it should address economic incentives by ensuring that equipment and technologies such as routers etc. can be implemented in an incremental manner, and changes to meet the dynamics of future attacks can be made quickly and easily at little to no cost.

There are various methods available to help you build a customized security solution that will increase your chances of not being hit by a Denial-of-Service or Distributed Denial-of-Service attacks. The solution will never offer 100% security! By designing suitably intelligent networks, considering both internal and external leased infrastructure, a company may never experience the problems associated with these attacks. ISP's are the best place to start offering protection for their customers against DDoS attacks. Many ISP's have special service offerings such as service level agreements with regard to response times [Arbor, 2005]. As customer you will receive early warning notifications of new attacks, and actions that should be taken by you. Security patches will be automatically sent to you. Honeynets are the greatest source of knowledge and they are currently working on setting up an e-commerce based scenario to trap attackers [Curran, 2005]. We need to setup different types of Honeynets in university labs across the world, this will increase our understanding, help us to see any changes in attack tools, methods or effects, and enable us to work together in finding and stopping them.

7 CONCLUSION

The way we do business and live our daily lives has changed due to the advances in networks and by the way in which we all communicate. The Internet and E-mail services nowadays are being used to a much greater extent. Banks offer online banking including money transfers and account payments, Universities allow online studying and retailers are doubling profits through online purchases. Families overseas can stay in touch with loved ones on a daily basis via online chat facilities. The problem is, there are loads of vulnerable systems connected to the Internet and any or all of these can be used as a launch pad for Denial-of-Service attacks, the effects of which could be devastating. The Internet is essentially a chain of networks and therefore only as strong as its weakest link. Distributed Denial-of-Service attacks are becoming extremely popular and common due to the effectiveness of this type of attack and the fact that the attackers are well hidden, therefore seldom caught.

The cost of performing an attack is low and the benefits high compared with those of defending a network. There are many reasons why attacks are not reported, perhaps it is too time consuming, or blackmail is involved, or there is fear of losing both existing and new clients by bad publicity. Although this makes it difficult to identify the extent of damage and number of occurrences, most surveys show that the top source of financial loss in cyber crime is a result of these attacks. New laws in the US and other countries require organizations to better protect the privacy of sensitive and personal information. Terrorist and criminal activity, directed at communications networks and computer systems, are growing. Cyber attacks and hacking are easier for a larger number of perpetrators due to increased use in Internet technology and connectivity around the world.

All the issues discussed in this paper need to be addressed at a global level, using all available resources. By examining the reasons why difficulties in defending these attacks exist, we can propose solutions based on our analysis. The conclusion we reached is that a distributed attack requires a distributed response! No single solution can guarantee protection but when implemented together in the correct fashion across the Internet we can certainly prevent a huge loss in the economy. Become knowledgeable about how these attacks could affect you and what part you can play in preserving the Internet's security and possibly our future way of life.

BIBLIOGRAPHY

AINSLIE, James. 2004. *Distributed Denial-of-Service: the Internet as a war zone.* Website Magazine Article. Retrieved: 3, April, 2005 from http://networktimes.co.za

ARBOR Networks. 2005. *Worldwide ISP Security Report*. Website Report. Retrieved: October 2005 from http://www.arbor.com.

CERT. 2001. Trends in Denial-of-Service Attack Technology. Retrieved April 2005 from www.cert.org/archive/pdf/DoS_trends.pdf

Cisco Systems Inc. 2001. *Economic Impact of Network Security Threats*. White Paper. Retrieved: March 21, 2005, from http://www.cisco.com/warp/public/cc/so/neso/sqso/roi1_wp.pdf

Cisco Systems Inc. 2005, *DDoS Prevention*. Website information. Accessed July 2005 at http://www.cisco.com.

CURRAN, Kevin et al. 2005. Monitoring hacker activity with a Honeynet. *Int. J. Network Mgmt*. 15 123 -134.

GARVEY, M. 2005. *Increasing Viruses Cause More Downtime*. Website Article. Retrieved 8 April 2005 from http://informationweek.securitypipeline.com/shared/article.

HOULE, K & WEAVER, G. 2001. *Trend in Denial-of-Service Attack Technology.* CERT/CC White Paper, vs1.0. Retrieved 15 April 2005 from http://cert.org/archive/pdf.

HOUSEHOLDER, A et al. 2001. *Managing the Threat of Denial-of-Service Attacks*. White Paper, vs. 10.0. Retrieved: 15 April 2005, from http://www.cert.org/archive/pdf/Managing_Denial-of-Service.pdf.

HUSSAIN, A et al. 2003. A Framework for Classifying Denial-of-Service Attacks. *Proceedings of SIGCOMM AUG '03 Germany*. 99 -110

LIBBENGA, J. 2005. *Dutch Hackers sentenced to attack on government sites.* Article. Retrieved April 2005 from http://www.tgeregister.co.uk/2005/03/16/dutch_hackers_sentenced.

MIRKOVIC, Jelena, REIHER, Peter. 2004. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. *ACM SIGCOMM Computer Communications Review*. 34 (2) 39 -54.

PATRIKAKIS, C, et al. 2004. Distributed Denial-of-Service Attacks. *The Internet Protocol Journal*, Cisco Systems Inc. 7(No. 4, December). 13-32.

PFLEEGER, C & PFLEEGER, S. 2003. *Security in Computing*. 3rd Edition. Prentice Hall.

SPEECHT, Stephen and LEE, Ruby. 2004. Distributed Denial-of-Service: Taxonomies of Attacks, Tools and Countermeasures. *International Conference on Parallel and Distributed Computing Systems*. 543 -550.

The SANS TM Institute. 2000. *Consensus Roadmap for Defeating Distributed Denial-of-Service Attacks*. Roadmap vs. 1. Retrieved 29 June 2005 from http://www.sans.org/dosstep/roadmap.php.

Tumbleweed. 2005. Dark Traffic E-mail Report Q3. Retrieved 3 May 2005 from: *http://www.tumbleweed.com/pdfs/ TMWD_Dark_Traffic_E-mail_Report_Q3_2005.pdf*