Introduction
The Internet is an open communication medium whose communications protocols were not designed to be security conscious, exposing the Internet to attack by anyone with basic computer skills. There are numerous threats on the Internet; however, this paper will focus on a particular attack known as the Denial of Service (DoS) attack. Denial of service attacks have been successfully and routinely launched against Internet-based services with high-profile attacks, occurring recently against Twitter and Facebook, making DoS attacks an important issue for anyone involved in the Internet industry. According to the 2004 CSI/FBI Computer Crime and Security Survey, DoS attacks are the most financially expensive type of security incidents faced by corporations providing Internet services. The same report listed DoS attacks as the second most prevalent attack against computers behind only virus attacks. Unfortunately, DoS attacks are likely to continue to increase in their frequency due to the ease of acquiring attack tools, their ease of use, and the availability of automated attack tools. (1)

Denial-of-Service attacks are not a new phenomena, this type of attack has “been a serious Internet threat for at least a decade.” (2) Public awareness of DoS attacks; however, has intensified due to the increased reliance on the Internet for “everyday communications, business tasks and even critical services such as vessel navigation, emergency service coordination, etc.” (2) A partial list of high-profile attacks this year includes:

March

GoGrid.com, a cloud computing provider disrupting service to ½ of its customers

April

Register.com, a Web hosting provider and one of the Internet’s largest domain name registrars.

The Planet, the world’s largest privately held dedicated Web hosting provider

Telefonica, an ISP in Brazil affecting 2.1 million users

May

SharkTech Internet Services, ironically a provider of anti-DDoS services to businesses, was knocked offline for five hours by an attack that sent more than 20 Gbit of traffic per second to the company’s servers, roughly the equivalent of the data contained in 5,000 novels per second. (3)
As with most security incidents on public corporations’ infrastructure, it is reasonable to assume that reported attacks represent some percentage of total attacks, but not all. (4) Therefore, the economic and social costs as well as the continuing threat posed by DoS attacks is sufficiently significant to warrant efforts to detect and mitigate these attacks by leaders in the industry.

This paper will provide a discussion of Denial of Service attacks defining what constitutes a DoS attack, and a sampling of the various methods used by DoS attacks to disable Internet services.

Denial of Service Attacks

In this case, a name says it all: denial of service. A DoS attack is launched for a singular purpose; that is, to encumber the resources of an Internet-based service denying legitimate users of its use. A formal definition of DoS attacks is provided by Carnegie Mellon’s Computer Emergency Response Team known as CERT:

“Occupancy of limited resource or difficult to renew [sic] such as bandwidth, data structure or memory of a system.

Changeable or damage network data, for instance delete system configuration, shutdown web service.

Changeable or damage physical information, for example damage of electronic, network line.” (5)

Another, arguably more direct definition is provided by Weiler:

“To inhibit legitimate network traffic by flooding the network with useless traffic.

To deny access to a service by disrupting connections between two parties.

To block access of a particular individual to a service.

To disrupt the specific system or service itself.” (6)

Several classification systems have been developed to describe forms of DoS attacks (1), this paper will not attempt to characterize DoS attacks, instead reporting on general classes of attacks. A DoS attack can be as simple as “flooding” an Internet service with a torrent of traffic, the attack may take advantage of a flaw in an application or the underlying communications protocol, or some combination of the three. A Flood attack swamps the Internet service provider with “a large, occasionally continuous, amount of network traffic workload.” (4) A Flood attack does not necessarily take
advantage of any weaknesses or flaws, it simply overloads the network and computing resources of the Internet service provider causing legitimate users to be blocked from using the service. In contrast, an attack that takes advantage of a flaw, a vulnerability attack, may send malformed messages, take advantage of a protocol weakness, or an application bug. Vulnerability attacks need not be high-volume, yet may result in “excessive memory consumption, extra CPU processing, system reboot, or general system slowing.” (4) The main advantage for the attacker in launching a vulnerability attack is that sending only a few packets can cause considerable damage. (7)

Nearly 90% of all Internet messages are formatted to conform to the TCP protocol. (8) So, it comes as no surprise that some vulnerability attacks are waged against the TCP protocol on which the Internet is dependent. A common form of TCP attack, the SYN attack, takes advantage of the “three-way handshake” that is the basis of establishing the TCP connection between two computers. In a normal TCP connection scenario a requestor sends a TCP SYN message to an Internet service provider, the service provider responds with a SYN ACK message at the same time creating and storing a connection, the requestor responds with an ACK message when received by the service provider the stored connection is retrieved and the connection process is complete. The vulnerability exploited by the TCP SYN attack sends the service provider a TCP SYN message with a spoofed requestor IP address thus causing the service provider to generate a SYN ACK message, create and store a connection for a requestor that does not exist and from which it will never receive the necessary final ACK message. The service provider’s resources become overwhelmed with pending TCP connection requests causing it to fail.

The TCP SYN attack is only one of many vulnerability attacks, other forms include the Smurf Attack which takes advantage of ICMP, Process Table and SSH Process Table, DoSNuke, ARP Poison, and others. Although some of the vulnerabilities may be closed by software patching, the underlying protocols on which the Internet is dependent cannot be modified instead they require distinct mitigation techniques. However, as the industry develops mitigation techniques for specific vulnerability attacks the attackers develop new and improved methods of disruption thereby perpetuating the cycle.

Mitigation of a DoS attack is not a matter of providing more computing horsepower or greater bandwidth because DoS attacks can be launched by a single person or by a group of people (9), the largest DoS attacks now exceed 40 Gigabits per second which easily overwhelms any service provider’s infrastructure. (10) Furthermore, if a single attacker is unable to succeed many other attackers may join in the attack or unsuspecting Internet users are enlisted remotely in the attack. In this scenario where an attack is launched from numerous geographically dispersed computers coordinating to disrupt a service, the attack is referred to as a Distributed Denial-of-Service attack (DDoS).

**Distributed Denial of Service Attack**
For an attacker, success is measured not only in the ability to deny services to legitimate clients, but also of not being caught in the act. (7) A DDoS attack provides an attacker the benefit of anonymity and the ability to mount a large-scale attack. To achieve these goals a DDoS attack requires the attacker to
“recruit” computers, unbeknownst to the owner (the recruitment or deployment phase), and launching the attack (the attack phase). (7) (11) In the deployment phase an attacker distributes a DDoS program onto the recruited computers, referred to as zombies, when some number of zombies are recruited their collection is referred to as an army. (9) In order to maintain anonymity the attacker controls the zombie army from one or more “master” zombies; a recruited computer which controls a portion of the attacker’s army. Now, with the army poised for the offensive, the attacker sends a command to the master zombies who, in turn, send commands to the zombie machines to activate the DDoS programs directing an attack toward the targeted Internet service. DDoS attacks are, generally, flooding attacks; however, the distributed nature of the attack amplifies its effect as is demonstrated in Figure 1.

![Figure 1: A typical DDoS attack](image)

Detection and mitigation of a DDoS attack is arduous because the traffic is being generated by a geographically dispersed group of computers, the DDoS attack has to be detected in real-time, and the traffic generated by the attack may not be distinguishable from legitimate “flash” traffic. (12) Considering that the Internet depends on the large-scale interconnectivity among computers, any server becomes an attractive target and any computer a potential zombie to a motivated attacker. Paul Lappas, vice president of engineering for GoGrid.com, describes the attack against his company, “the attack came from thousands of servers around the Web, and targeted every last one of the company’s Internet addresses.” He continues, “Our systems were designed to handle extremely large DDoS attacks. We’ve been in this business for eight years, and seen our share of attacks. But we haven’t seen anything like this before.” The attack against GoGrid.com lasted for several days ending as abruptly as it began. (3)

**Summary**

As attackers form their armies for sieges against unsuspecting Internet service providers, a counter force exists to thwart their efforts. If the goal of an attacker is to deny service, then the goal of defenders is to
mitigate the “impact of the attack on the victim while imposing minimal collateral damage to legitimate clients.” (11) Because the Internet does not discriminate when forwarding traffic, distinguishing between attack traffic and legitimate traffic hampers the efforts to detect and mitigate an attack. Current detection methods rely on statistical comparisons of network traffic against “normal” measured traffic flow which, unfortunately, does not account for sudden increases in legitimate traffic thereby producing an inordinate number of false alarms. As the battle continues, innovative approaches are emerging which incorporate advanced statistical methods and application of digital signal processing techniques such as spectral analysis and wavelet analysis to the detection of DDoS attacks in a concerted effort to gain an advantage against the attackers.

Although the Worldwide Infrastructure Security Report declares that the level of concern related to DDoS flooding attacks is down for a variety of reasons (10) there remains significant concern associated with other DDoS vulnerabilities. Laurens, et al. argues that DDoS techniques are quickly evolving to take advantage of new vulnerabilities discovered in the Internet infrastructure (7) such as the Kaminsky DNS attack. “Attackers manage to discover other weaknesses of the protocols and – what is worse – they exploit the defense mechanisms in order to develop attacks.” (9) The consequences of the economic and social devastation caused by DoS attacks ensure that efforts to defend against and mitigate these attacks will endure.
References


